Theses and Dissertations   1. Thesis and Dissertation Collection, all items

2008-09

An ontological approach to developing Information Operations applications for use on the semantic web

Clarke, Timothy L.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/3940

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN ONTOLOGICAL APPROACH TO DEVELOPING INFORMATION OPERATIONS APPLICATIONS FOR USE ON THE SEMANTIC WEB

by

Timothy L. Clarke

September 2008

Thesis Advisor: Man-Tak Shing
Co-advisor: Karl Pfeiffer

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.		
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis
4. TITLE AND SUBTITLE An Ontological Approach to Developing Information Operations Applications for use on the Semantic Web		**5. FUNDING NUMBERS**
6. AUTHOR(S) Clarke, Timothy L.		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.		
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Information Operations (IO) have the potential to alter the landscape of modern warfare through the sustained application of a broad spectrum of kinetic and non-kinetic effects. Operations of this type offer the benefit of reducing the scope of direct conflict by shaping the perceptions of a potential adversary. The complexity and diversity of IO makes it an ideal beneficiary of software applications, but current systems have yet to truly leverage domain expertise in systems development. By expressing IO capabilities in a formal ontology suitable for use on the Semantic Web, conditions are set such that computational power can more efficiently be leveraged to better define required capabilities and more reliably predict effects.

The purpose of this thesis is to identify gaps in existing IO software applications, demonstrate how IO capabilities may be represented in a software ontology, and develop a process by which an IO ontology may be adapted for use on the Semantic Web. These objectives are accomplished by examining leading IO applications, demonstrating a process for converting the IO problem domain into an ontology using the Protégé 3.3 Ontology Editor, and assessing the suitability of the ontology for use on the Semantic Web.

14. SUBJECT TERMS Information Operations (IO), Psychological Operations, PSYOP, Electronic Warfare (EW), Electronic Attack (EA), Electronic Protect (EP), Electronic Support (ES), Semantic Web (SW), Resource Description Resource (RDF), Ontology, Ontology Web Language (OWL), Protégé, Poseidon		**15. NUMBER OF PAGES** 147
		16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

AN ONTOLOGICAL APPROACH TO DEVELOPING INFORMATION OPERATIONS APPLICATIONS FOR USE ON THE SEMANTIC WEB

Timothy L. Clarke
Lieutenant Colonel, United States Marine Corps
B.S., Truman State University, 1992

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT
and
MASTER OF SCIENCE IN SOFTWARE ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2008

Author: Timothy L. Clarke

Approved by: Man-Tak Shing
                   Thesis Advisor

                   Karl Pfeiffer
                   Co-Advisor

                   Peter Denning
                   Chairman, Department of Computer Science

                   Dan Boger
                   Chairman, Information Sciences Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Information Operations (IO) have the potential to alter the landscape of modern warfare through the sustained application of a broad spectrum of kinetic and non-kinetic effects. Operations of this type offer the benefit of reducing the scope of direct conflict by shaping the perceptions of a potential adversary. The complexity and diversity of IO makes it an ideal beneficiary of software applications, but current systems have yet to truly leverage domain expertise in systems development. By expressing IO capabilities in a formal ontology suitable for use on the Semantic Web, conditions are set such that computational power can more efficiently be leveraged to better define required capabilities and more reliably predict effects.

The purpose of this thesis is to identify gaps in existing IO software applications, demonstrate how IO capabilities may be represented in a software ontology, and develop a process by which an IO ontology may be adapted for use on the Semantic Web. These objectives are accomplished by examining leading IO applications, demonstrating a process for converting the IO problem domain into an ontology using the Protégé 3.3 Ontology Editor, and assessing the suitability of the ontology for use on the Semantic Web.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGMENTS

With foremost appreciation to the wisdom and tutelage of my mentors and the patience and understanding of my family.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The dogmas of the quiet past are inadequate to the stormy present. The occasion is piled high with difficulty, and we must rise with the occasion. As our case is new, so we must think anew and act anew.

Abraham Lincoln
Message to Congress, 1 December 1862

A. THE INFORMATION OPERATIONS SOFTWARE CHALLENGE

Information Operations (IO) have the potential to alter the landscape of modern warfare through the sustained and prudent application of a broad spectrum of kinetic and non-kinetic effects. Operations of this type offer the benefit of reducing the scope of direct conflict by shaping the perceptions of a potential adversary. Within the Department of Defense, IO has matured unevenly. Various IO capabilities are segmented within each of the respective services, assets are procured via service channels, there is no single overarching authority, and IO is often viewed with apprehension by the larger military community. The complexity and diversity of IO makes it an ideal beneficiary of software applications, but current systems have yet to truly leverage domain expertise in systems development. By expressing IO capabilities in a formal ontology suitable for use in the Semantic Web, conditions are set such that computational power can be leveraged to better define required capabilities and more reliably predict effects.

As espoused by Sun Tzu, the acme of skill is to achieve victory without engaging in armed conflict. In a more modern context IO provides a means by which this can realistically be accomplished, but not without a considerable degree of foresight, a clear understanding of the consequence of action, a realistic assessment of the limitations of the resources available, and a holistic view that gives consideration to the longer term impacts. Succinctly, effective IO is a difficult undertaking. The resulting question is how to conduct IO in a more effective and predictable manner. One possible solution lies in the use of computer applications optimized for IO planning and execution. The purpose of this thesis is to demonstrate how the IO problem domain can be formalized

1

into an ontology suitable for use in the Semantic Web in order to facilitate more effective IO campaigns. This will be accomplished by answering the following questions:

1. What are specific gaps in existing Information Operations (IO) software applications?

2. How can IO capabilities be represented in a formal software ontology?

3. What is the process by which an IO ontology may be adapted for use on the Semantic Web?

To answer these questions, this thesis will examine leading IO applications, demonstrate a process for converting the IO problem domain into an ontology using the Protégé 3.3 Ontology Editor developed by the Stanford University School of Medicine, and assess the suitability of the ontology for use on the Semantic Web. As the Protégé editor allows for files to be exported in both Resource Description Framework (RDF) and Ontology Web Language (OWL) formats, it is envisioned that through the use of Hewlett Packard's Jena Semantic Web Toolkit the IO ontology can be readily adapted for use on the Semantic Web.

B.   IO: THE PROBLEM DOMAIN

IO encompasses numerous disciplines, to include Psychological Operations, Military Deception, Operations Security, Electronic Warfare, and Computer Network Operations.   Additionally, there are eight other related and supporting disciplines consisting of: Defense Support to Public Diplomacy, Civil Military Operations, Public Affairs, Information Assurance, Combat Camera, Counter Intelligence, Physical Attack, and Physical Security. Conceptually, the optimal application would be able to model the characteristics of each discipline and, given a defined set of objectives and regionally specific information, provide the most effective means of achieving the greatest effect with a minimal application of force.

The IO problem domain is well served by a significant number of doctrinal publications. Joint Publications as well as numerous service publications and popular literature all provide a point of departure for examining the respective disciplines that

cumulatively form IO. From the perspective of ontological development, this offers the advantage of a mature and well-documented problem domain with an established knowledge base which can be deconstructed and rebuilt into an ontology. It is worth noting, though, that the publications were written to convey concepts between people, not machines. The following excerpt from JP 3-13: Information Operations captures the essential interactions, relationships and complexity of IO:

> The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The actors include leaders, decision makers, individuals, and organizations. Resources include the materials and systems employed to collect, analyze, apply, or disseminate information. The information environment is where humans and automated systems observe, orient, decide, and act upon information, and is therefore the principal environment of decision making. Even though the information environment is considered distinct, it resides within each of the four domains. The information environment is made up of three interrelated dimensions: physical, informational, and cognitive.

The final sentence of the preceding excerpt is critical in understanding what IO is intended to achieve. The use of the multiple disciplines of IO to achieve an effect is not unlike the well-established and long-used practice of combined arms, the key distinctions in IO are the dimensions over which the effects are realized. Unlike more traditional operations, which result in the capitulation of an adversary, IO adopts a broader approach aimed at shaping an adversary's thought process through the combined effects of operations in both tangible and intangible domains. The following are the doctrinal definitions of the dimensions in which IO exists:

1.   The Physical Dimension

The physical dimension is composed of the command and control (C2) systems, and supporting infrastructures that enable individuals and organizations to conduct operations across the air, land, sea, and space domains. It is also the dimension where physical platforms and the communications networks that connect them reside. This includes the means of transmission, infrastructure, technologies, groups, and populations.

Comparatively, the elements of this dimension are the easiest to measure, and consequently, combat power has traditionally been measured primarily in this dimension. (JP 3-13)

2. The Informational Dimension

The informational dimension is where information is collected, processed, stored, disseminated, displayed, and protected. It is the dimension where the C2 of modern military forces is communicated, and where commander's intent is conveyed. It consists of the content and flow of information. Consequently, it is the informational dimension that must be protected. (JP 3-13)

3. The Cognitive Dimension

The cognitive dimension encompasses the mind of the decision maker and the target audience (TA). This is the dimension in which people think, perceive, visualize, and decide. It is the most important of the three dimensions. This dimension is also affected by a commander's orders, training, and other personal motivations. Battles and campaigns can be lost in the cognitive dimension. Factors such as leadership, morale, unit cohesion, emotion, state of mind, level of training, experience, situational awareness, as well as public opinion, perceptions, media, public information, and rumors influence this dimension. (JP 3-13)

As these definitions illustrate, IO reconsiders the battlespace in a broader context. By shaping the perceptions of an adversary, conditions are established such that conflict may be deterred, shortened, or less destructive. All of these effects are desirable and are representative of a fundamentally more efficient means of waging war.

C. THE SOFTWARE DEVELOPMENT PARADIGM

Software development has historically been a somewhat haphazard undertaking. While there are notable successes, there have historically been far more software

failures.[1] This implies that the method used in the development of software is of significance in its own right, and should be considered not just in the context of process efficiency, but also in the context of the problem domain it is envisioned to support. In considering viable approaches for developing IO applications, an ontological approach offers great potential in that it lends itself to defining relationships between actions and behavior in a manner such that computers can more readily be employed in support of operations. The following definition is extracted from the Protégé project:

> Ontology: An ontology describes basic concepts in a domain and defines relations among them. Basic building blocks of ontology design include classes or concepts, properties of which describe various features and attributes of the concept and role restrictions. An ontology together with a set of individual instances of classes constitutes a knowledge base. An ontology provides a common vocabulary for researchers who need to share information in the domain. Reasons for creating an ontology are to share a common understanding of the structure of information among people or software agents, to enable reuse of domain knowledge, to make domain assumptions explicit, to separate domain knowledge from operational knowledge, to analyze domain knowledge.

The exponential growth of available information has introduced new challenges in the field of knowledge management. Ontology based techniques have gained increasing acceptance as a means for managing knowledge by facilitating tagging and semantic searches. The use of ontologies to formally define the terms and relationships within various problem domains offers a variety of potential benefits. Through the use of a common set of standardized definitions and hierarchies, both people and software agents are better positioned to achieve a shared understanding of a given domain. Further, an ontological approach to software development also offers a heightened potential for reuse, provides more explicit definitions of terms and relationships, and increases the ease of analyzing domain knowledge. Succinctly, ontologies offer the potential to overcome barriers created by disparate vocabularies, representations and tools. While

---

[1] Jones, C. "Patterns of Large Software Systems: Failure and Success." *Computer* 28, no. 3 (1995): 86-87.

there is a litany of potential applications for this approach, the intent of this document is to examine the benefit of ontologies in regards to the development IO applications for the Semantic Web.

The partial IO ontology will be developed using the Protégé 3.3 Ontology Editor developed by the Stanford University School of Medicine. Through the use of this tool, it is expected that the concepts and capabilities of IO can be expressed with sufficient formalism to be suitable for use with the Semantic Web. The ontology will consider the full range of IO capabilities, but at this time Psychological Operations (PSYOPS) and Electronic Warfare (EW) are being considered as primary areas of emphasis within the ontological development. IO is ultimately a concept centered on influencing the cognitive, decision-making process of an adversary. The combination of PSYOPS and EW intuitively provides a means to shape perceptions and a mechanism to control several means of dissemination. In this regard, some elements of synergy can conceivably be achieved although all IO disciplines are not employed.

D.   THE SEMANTIC WEB

The final element of this initiative is assessing the suitability of the ontology for use on the Semantic Web. As the Protégé editor is designed to craft ontologies for use on the Semantic Web, it allows for files to be exported in both Resource Description Framework (RDF) and Ontology Web Language (OWL) formats. It is envisioned that through the use of Hewlett Packard's Jena Semantic Web Toolkit the IO ontology can be readily adapted for use on the Semantic Web. Note that a fully functioning IO application will not be developed as a result of this thesis. The intent is to illustrate and define a methodology for adapting IO concepts and capabilities for use on the Semantic Web.

E.   THE WAY AHEAD

One of the most recurring software challenges we face is the seam between how humans perceive the world and how machines interpret our perceptions. IO resides largely in the cognitive domain, and as a result any meaningful application must be able to consider the battlespace in a consistent and accurate manner. Ontologies offer the

potential to frame IO in such a context that the gap between man and machine is further narrowed. The Semantic Web makes the ontology useful to a broader audience. This thesis will frame a methodology for deconstructing elements of the IO domain and reinterpreting it as an ontology suitable for use on the Semantic Web.

F.   THESIS ORGANIZATION

Chapter I provides an introduction that includes an overview of the problem to be addressed, the nature of the IO problem domain, an examination of the current software development paradigm, the potential of the Semantic Web, the merging of IO and the Semantic Web, and the organization of the thesis document.

Chapter II provides a review of related literature. This review examines a variety of recent documents addressing the development of software ontologies, information operations, and the Semantic Web. These documents are considered in the context of their relevance to this thesis.

Chapter III examines the current state of automated support to IO, with an emphasis on the Information Warfare Planning Capability (IWPC). This examination addresses the relative strengths and weaknesses of the applications comprising IWPC and identifies means by which the Semantic Web may improve upon the current state of practice.

Chapter IV analyzes selected elements of the IO problem domain, specifically capabilities and platforms associated with psychological operations and electronic warfare. This analysis provides the basis on which the ontology will subsequently be developed.

Chapter V takes the domain analysis and translates it into a partial ontology of the IO domain. The selected elements of IO are first considered in a manner that establishes key levels of aggregation and the nature of interactions. These are then entered into the Protégé ontology editor. This is followed by a series of tests, the development of multiple views, and the export of the Protégé files to a Unified Modeling Language (UML) editor.

Chapter VI takes the actions executed in the preceding chapters and establishes them in a more definitive methodology. This methodology consists of seven general steps that, while applied in the IO domain, are broad enough to have wider utility.

Chapter VII discusses the conclusions of this thesis, the broader impacts of semantic militarization, the doctrinal impacts of such a shift, the role of ontologies and the criticality of well defined rule-sets. The chapter ends by a offering recommendations for future work.

Appendix A consists of selected elements of the IO problem domain expressed in the Ontological Web Language (OWL).

Appendix B consists of selected elements of the IO problem domain expressed in JAVA schema.

II. REVIEW OF RELATED LITERATURE

Military professionals must know something about strategy and tactics and logistics, but also economics and politics and diplomacy and history. You must know everything you can about military power, and you must also know the limits of military power. You must understand that few of the problems of our time have been solved by military power alone.

John F. Kennedy
Address at the U.S. Naval Academy Commencement, June 7, 1961

A. CONTENT OF THE REVIEW

This review of related literature is divided into four sections reflecting the broader context of this thesis. The first section, Information Operations (IO), examines the doctrinal definitions and concepts surrounding IO. The references in this section explore the IO problem domain from both a doctrinal and practical perspective which collectively serves to establish the basis on which the ontology will be developed. The second section, Software Ontologies, examines current methodologies for developing ontologies. The variety of approaches to ontological development contained in these references lend themselves to the development of a hybrid approach specifically oriented towards the IO domain. The third section examines key points in developing applications and prevailing wisdom on the potential of the Semantic Web. Given that the ontology is effectively a means of translating domain knowledge into an application suitable for use on the Semantic Web, an understanding of best practices in this field is a necessary background for developing ontologies of broad utility. The final section concludes with a brief summary of the review of related literature, highlighting key elements of each section and addressing any significant gaps that may adversely impact the development of this thesis.

B. SOFTWARE ONTOLOGIES

The acquisition of sufficient domain knowledge represents the first step in developing a useful ontology, but the mechanics of translating this knowledge into a meaningful, useful, and technically accurate ontology presents quite another challenge.

In order to determine the best practices for ontological development, literature from a variety of sources was reviewed. It should be noted that the selection of Stanford's Protégé ontology editor as the development tool defined a great deal of the methodology. In order to employ the tool to optimum effect, significant weight was given to the recommendations found in the Protégé tutorials.

A great deal of the promise of ontological development lies in its relation to the semantic web. In his article "A Flexible Ontology Reasoning Architecture for the Semantic Web," author Jeff Pan offers a conceptual framework for linking the two. The author begins with OWL-Eu and OWL-E, extensions of the standard ontology language OWL DL, and proposes a reasoning architecture for these two ontology languages. The key features of the author's architecture are that it allows users to define their own data types and data type predicates based on existing ones and it allows for new data type reasoners to be added into the architecture without having to change the concept reasoner. A key component of this approach is flexibility which is of significant benefit in tailoring an application to an adaptive or rapidly changing environment. This feature has a great deal of potential for conducting operations in an information environment.

Another arena that stands to benefit from ontological development is software reuse. In the context of reuse, a hierarchical ontology offers the benefit of logically organizing software components within the domain model, lending itself to both an understanding of how the component is utilized and rapid cataloging. In their article "Developing Software for and with Reuse: An Ontological Approach" authors Falbo, Guizzardi, Duarte, and Natali illustrate this in the software quality domain. While an ontology for reuse will not mirror an ontology for IO, the methodology employed by the authors bears consideration for other problem domains. Further, incorporating reusable components in tailoring applications to meet specific operational needs offers the potential of both increased flexibility and speed in developing relevant software.

The utility of an ontology can be defined by the degree to which it accurately reflects its intended problem domain, and part of the promise of the ontological approach is narrowing the margin between the domain experts and the software developers. In their article "Ontology Building: A Terrorism Specialist's Perspective," authors Aaron

Mannes and Jennifer Golbeck discuss their methodology for developing their efforts towards defining terrorism in an ontology. While their objectives and motivations differ greatly from the U.S. military, terrorism often employs methods not dissimilar from IO. This article provides insight into both a relevant development methodology and applicable domain knowledge.

Not unlike other practices, ontological development benefits significantly from the use of various tools. In their article "A Tools Environment for Developing and Reasoning about Ontologies" authors Jin Song Dong, Yuzhang Feng, Yuan Fang Li, Jun Sun from the National University of Singapore examine the tools available for ontological development from the premise that the correctness of the ontology is the critical component underpinning the proper functioning of agents. The authors illustrate the process through which they developed an integrated tools environment to support the systematic development of OWL ontologies. In their tools environment, they employ a variety of applications which serve to support the underlying reasoning behind the ontology. The utility of this article stems from both the methodology described by the authors and the introduction of other ontology development tools. While their methodology will not be directly applied in this thesis, common elements will be found.

Not all authors view the future of ontological development in an optimistic light. In his article "Possible Ontologies: How Reality Constrains the Development of Relevant Ontologies" author Martin Hepp offers a critical examination of the obstacles of ontological development. The author identifies several areas that, in his opinion, are not sufficiently addressed in the current ontological development paradigm. Among these issues are concerns about the pace of ontological development and whether it is in fact responsive enough to reflect rapidly evolving domains. Economic incentives, issues surrounding intellectual property rights, and the potential gap between the ontology developer and the end user are also addressed. The author considers ontological development in a holistic fashion and the issues he presents will undoubtedly need to be addressed to realize the potential of the semantic web. Relative to this thesis, this article provides several potential challenges that should be considered in the development methodology.

The emergence of ontology development tools has also yielded several tutorials discussing best practices. In their primer "Ontology Development 101: A Guide to Creating Your First Ontology" authors Natalya Noy and Deborah McGuinness of Stanford University discuss both the utility of and methodologies for developing ontologies. Based on lessons learned using Protégé 2000, the authors examine all facets of the ontology and provide step by step instructions for its construction. Replete with several examples and diagrams and aligned with the Protégé development tool, this article serves as a strong tutorial on both development methodology and the use of the Protégé tool.

C. INFORMATION OPERATIONS

While several documents addressing IO will be reviewed in this section, Joint Doctrine provides the basic foundation. As a result, there tends to be very little incongruity or dissension as the terms, definitions, and concepts found in one joint publication are consistent with both other joint and service publications. While this approach does not readily accommodate more current publications on emerging IO concepts, it is necessary to establish the baseline from which the ontology will ultimately be developed. Absent this, relationships cannot be traced back to a doctrinal basis and have the potential to introduce inconsistency into the desired effects. Further, in the context of this thesis the purpose of reviewing IO literature is not to challenge any specific doctrinal concept, but to establish a baseline from which the ontology will ultimately be based.

The primary document reviewed for IO domain knowledge is Joint Publication 3-13: Information Operations. This text is absolutely essential for establishing an understanding of the vision for IO as conceived by the United States. It does not offer a great deal of depth on any single IO discipline, but it effectively captures the key facets of the IO environment in a structured manner that provides for the higher levels of abstraction in an IO ontology. While an understanding of all the concepts discussed in the publication is ultimately required, the sections addressing the information environment, core, supporting, and related IO capabilities, planning and coordination, and measures of performance and measures of effectiveness are all critical to this thesis

in that they offer a basis for objects, environment, and actions. Succinctly, this document frames the top-level ontological construct.

Joint Publication 3-53: Psychological Operations is also examined closely. As PSYOPS is one of the core capabilities being developed in the ontology, this publication provides the basis on which it is founded. While consistent with the information found in JP 3-13, it expands on the actual conduct and planning of psychological operations. The text contains relevant information on organizational responsibilities, command relationships, planning and approval, and respective service capabilities. Each of these facets is critical to understanding psychological operations and are thus essential to capturing relevant domain knowledge in an ontology.

IO is not undertaken as a monolithic entity, they span the range of the operational continuum. Turner (2005) proposes a methodology for generating IO synergy through integrating efforts at the strategic, operational, and tactical levels of war. This striated aspect of modern warfare is a significant consideration in examining the operational context of IO. The utility of this in developing an ontology is that it allows for a layer of abstraction centered around a set of effects focused on a given echelon of targets. While the joint publications offer definitions of the levels of warfare and encourage synergy between the three, this document offers a rationalized methodology for achieving this within the IO problem domain.

In his book, *Psychological Operations: Principles and Case Studies*, authors Frank Goldstein and Benjamin Findley provide critical examination of the United States conduct of PSYOPS in Vietnam, Libya, Panama, Iraq, and counter-drug operations. Attention is also given to PSYOPS in other parts of the world and in support of insurgencies. While steeped in the doctrine of the era, the text offers eight separate case studies analyzing various dimensions and effects of PSYOPS. This text proves to be an excellent supplement to the doctrinal publications in that it offers insight and nuance into how operations of this type manifest themselves in actual practice. In this capacity, it forces consideration of relevant factors that are not present solely in doctrine.

In a similar vein, Sokoloski (2005) offers a more progressive approach towards PSYOPS based on modern marketing principles. While this document is heavily steeped

in Army, vice joint, doctrine, what makes it notable is the degree to which it articulates shortfalls in existing PSYOPS practices and the potential solutions the author introduces. While some of what is suggested is well beyond what is found in joint doctrine, it speaks to the very practical issue of effective implementation of the concepts found in doctrine through otherwise non-traditional means. In the context of crafting a viable ontology, the value this brings is the introduction of another layer of relationships to add to both the versatility and utility of said ontology.

The Defense Science Board's report, "The Creation and Dissemination of All Forms of Information in Support of Psychological Operations (PSYOP) in Time of Military Conflict," also proves to be of great utility in defining PSYOPS in terms of the medium in which the message is delivered. The utility of this report relative to capturing the domain in an ontology stems from the level of abstraction at which the concept is presented. Whereas the aforementioned doctrinal publications and case studies tend to present operations in platform specific terms, this report considers operations in terms of media type. This is significant in that this level of abstraction is neither service nor platform specific and can be expressed in more absolute and enduring terms. This aspect of consistency is critical in considering ontological development as it presents a basis for relationships between sender and receiver that will hold true for the majority of information exchanges.

The concept of stable operational concepts from which an ontology can be built around is again explored is found again in Thomas (2006) thesis. This document introduces two case studies addressing influence operations, post-World War II Philippines and the Malayan Emergency of 1948-1960. Based on his examination of these cases, the author introduces eight principles of grassroots psychological operations. While these principles are generally consistent with the tenets espoused in both JP 3-13 and military operations in general, the utility lies in the terms in which they are expressed, the echelon at which they are employed, and their relation to cases in which influence operations were undertaken. In aggregate, this thesis offers additional perspectives and vantage points from which domain knowledge can be considered.

The United States is not the only entity that undertakes IO, so it stands to reason that there are numerous lessons to be learned from other practitioners. In their thesis *A Terrorist Approach to Information Operations*, Majors Robert Earl and Norman Emery consider IO from the perspective of terrorist organizations. While the motivations, resources, and tactics employed by terrorist organizations vary greatly from the United States, from both a PSYOPS and an ontological standpoint several insights can be gleaned from how they ply their trade. Of specific value is the means by which the authors characterize the audience of a terrorist's PSYOP message, adding another layer of abstraction to better define the full range of effects found in PSYOPS.

The intent of this thesis is ultimately to extricate the domain knowledge in IO, specifically PSYOPS, and present it in an ontology. The essence of this is ultimately presenting a subset of a larger military domain in ontological terms. To that end, the article "Study on Construction and Integration of Military Domain Ontology, Situation Ontology and Military Rule Ontology for Network Centric Warfare," by Song Jun-feng, Zhang Wei-ming, Xiao Wei-dong, Xu Zhen-ning provides an example of an approach taken towards capturing military domain knowledge in an ontology. While the examples provided by the authors are steeped in conventional capabilities such as fighter planes and radar, the methodologies employed have the potential for much broader application, to include IO.

Collectively, these works provide the basis for defining the problem domain. This ensures that the ontological framework is grounded in terms of the human understanding of IO and IO sub-disciplines. Absent a definitive link to a source interpretable and accepted by humans, there is no basis on which the ontology can be built. As one of the fundamental objectives of the Semantic Web is to facilitate greater machine understanding of concepts, it becomes critical that the human understanding is faithfully represented. These works are useful to this thesis as they provide the basis of human understanding of the IO discipline.

D.   SEMANTIC WEB

The utility of ontological development is linked closely to its use on the semantic web. For that reason, an understanding of the potential and limitations of what can

realistically be achieved on the semantic web is a worthwhile starting point. In their article "The Semantic Web: Prospects and Challenges" author's Michael Wilson and Brian Matthews examine the origins of the semantic web, the benefits that can be derived from its maturation, and the impediments that need to be overcome to realize its full potential. The authors consider the challenges of ontological modeling, logical basis for inference, translating between ontologies and the impacts of metaphors, reasoning about intentions, and the sociology of agents. The challenges identified by the author all speak to the problems associated with logical consistency when this is not often the case with any number of exchanges. Succinctly, the issues addressed in this article are directly applicable to building a sound ontology which in turn becomes a viable entity on the semantic web.

The potential of the Semantic Web will not be realized independent of current practices. To some extent, existing database content will be necessary to support Semantic Web applications. Authors Dejing Dou, Paea LePendu, Shiwoong Kim, and Peishen Qi explore this practical consideration in their article "Integrating Databases into the Semantic Web through an Ontology-based Framework." The authors address the challenge of "supporting human experts in multiple domains to interactively integrate information that is heterogeneous in both structure and semantics." The approach taken by the authors entails the use of ontologies built to incorporate database schemas. Using the Web-PDDL ontology language, they define the structure, semantics, and mappings of data resources. They proceed to illustrate the effectiveness of this approach through two case studies contained within the article. In considering the challenges of Semantic Web applications in the IO domain, similar challenges will be faced in developing a means to incorporate data from a variety of disparate sources. The scope and information requirements of full-spectrum IO are such that the utility of supporting applications will be largely defined by the amount of data they can access and process. The authors present a viable approach for overcoming a significant portion of this challenge.

The utility of the Semantic Web in military operations is not a new concept. In their 2003 thesis, *Assessing the Potential Value of Semantic Web Technologies in Support of Military Operations*, author's Samuel Chance and Marty Hagenston consider this topic

in great detail. While the authors consider military applications in a broader context than strictly IO, their perspective is sufficiently holistic to encompass IO and examine the relationship between ontologies and the semantic web. The authors proceed to examine how Semantic Web technologies can be applied in a military domain and in doing so provide a point of reference from which IO applications may be considered.

Other authors have also considered the Semantic Web in terms of potential military applications. Childers (2006) examines the military potential of applying Semantic Web technologies to XML languages. She closely examines existing Semantic Web tools, ongoing Semantic Web projects, and the relationship between Artificial Intelligence and the Semantic Web. While there is a strong emphasis on the Tactical Assessment Markup Language (TAML), the methodology used by the author to formulate and test the TAML ontology offers key insights into a viable process that may be suitable for other applications, to include IO.

The potential utility of the Semantic Web is much greater than the military domain. In their article "A Survey on Semantic Web Services and a Case Study" authors Jiehan Zhou, Juha-Pekka Koivisto, and Eila Niemela survey Semantic Web services from the viewpoints of web service architectures, service engineering, service description languages, and web service building tools. By adopting a broad perspective, the authors illuminate key areas of development that must be addressed to realize the potential of the Semantic Web. Further, through the use of a case study the authors present an example of the challenges and solutions surrounding the integration of a variety of web services. The value of the Semantic Web will not be realized solely through military applications, the commercial sector will also reap the benefits of its use. This article is of benefit to this thesis as it illustrates approaches taken outside the military domain and offers a broader perspective of the challenges at hand.

The essence of crafting applications for the Semantic Web is software development. Resultantly, the discipline and tools of Software Engineering lend themselves to a reasoned approach towards developing Semantic Web applications. In their article "Software Engineering Approaches to Semantic Web," authors J. S. Dong and D. Dan discuss the potential role of Software Engineering in Semantic Web development. The authors also examine the relationship between ontologies and the

Semantic Web, asserting that "in the development of Semantic Web there is a pivotal role for ontology, since it provides a representation of a shared conceptualization of a particular domain that can be communicated between software programs. As autonomous software web agents may need to make their own decisions based on their knowledge, it is essential that the shared ontology is consistent." Given the importance of consistency in the ontology, the authors advocate the use of software engineering techniques and tools to complement the ontology tools for checking Semantic Web documents. This aspect of ontological consistency is essential to sound ontologies and the methods proposed by the authors offer another perspective on how to achieve this.

To achieve optimum results, numerous tools focused on a variety of effects at various levels of warfare must be employed. In a similar fashion, one of the challenges facing the Semantic Web is its ability to operate across multiple problem domains. In their article "Towards a Multi-Domain Semantic Web Application," authors Anwar Hossain, Abdulmotaleb El Saddik, and Pierre Levy address this challenge by developing a multi-domain Semantic Web application intended to provide a collective intelligence model of society. Emphasizing domains the authors refer to as people, document, technical, knowledge, intentions, and skills, they introduce a high level infrastructure aimed at implementing their model on the Semantic Web. While the model developed does not present a developed ontology of the previously mentioned domains, the article contains a Collective Intelligence model that highlights key interactions. Given the parallels between the domains explored by the authors and the domains comprising IO, the article provides a framework that may be suitable for broader application.

E.   SUMMARY

In aggregate, the works identified provide a basis for defining selected elements of the IO problem domain, structuring these elements into an ontology representative of the basic rules of their interaction, and generating an output that is suitable for use on the Semantic Web. This contributes to the collective body of IO and Semantic Web knowledge in that it offers an interpretation of the underdeveloped IO problem domain in a form adhering to Semantic Web principles. In doing so, conditions are set for expanding the depth of the Semantic Web as a new domain is expressed in machine understandable terms.

III.   STATE OF THE PRACTICE

In the practical art of war the best thing of all is to take the enemy's country whole and intact; to shatter and destroy it is not so good. Hence, to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting.

Sun Tzu

A.   INFORMATION WARFARE PLANNING CAPABILITY

Harnessing computing power in support of IO presents significant difficulties. The breadth of full spectrum IO encompasses a diverse range of core, supporting, and related capabilities, many of which are complex disciplines in their own right. Developing a single application capable of fully addressing the unique requirements of multiple disciplines, facilitating increased operational synergy, and adapting to continuously changing conditions in a problem domain that is largely cognitive introduces considerable challenges.

While many of IO's sub-disciplines have successfully employed computer applications for quite some time, they have enjoyed the advantage of being focused on a relatively small portion of battlespace activity. As an example, signal propagation software in support of Electronic Warfare (EW) has long been of benefit to EW practitioners, but these applications existed in a stovepipe environment precluding seamless integration with other warfighting functions. To some degree, this element of isolation precludes the type of synergy that IO seeks to achieve. This shortfall has been recognized and resulted in the development of the Information Warfare Planning Capability (IWPC).[2]

Originally developed by General Dynamics in support of the Air Force, IWPC represents the first significant step towards integrating support tools to better develop and execute full-spectrum IO, encompassing the full range of core, related, and supporting activities. As described by the developer, IWPC is "a suite of effects-based campaign

---

[2] General Dynamics Advanced Information Systems. *Information Warfare Planning Capability*. Online brochure. Arlington, VA: 2007. URL:<http://www.gd-ais.com>. Accessed May 24, 2007.

tools designed to provide collaborative information and decision support to warfighters during campaign planning and execution. The tools leverage a services-orientated architecture enabling dynamic planning, analysis, targeting and operations assessment." While IWPC represents a more evolved and comprehensive treatment of IO support applications, its utility is not unbounded. This chapter will examine the capabilities and limitations of IWPC in the context of how IO applications developed for the semantic web may be of greater utility.

B.   IWPC CAPABILITIES

While numerous commercially available applications support IO, only one was developed specifically for the conduct of information warfare. The Information Warfare Planning Capability (IWPC) began development in 2002 and is currently being employed within the United States Air Force. The focus of the system is to provide "a suite of collaborative tools supporting integration of kinetic and non-kinetic effects in operational planning and execution."[3] To achieve this, IWPC combines the numerous tools under the rubric of a single application. The following extracts from the IWPC program literature highlight its capabilities:

Collaborative Planning Tool (CPT): The CPT provides planners and targeteers a flexible planning capability to perform effects-based planning, to include effect chains and causal linkages. Through the use of CPT, planners are able to enter the commander's planning guidance, phases, objectives and desired effects, and subsequently decompose the objectives and effects into actionable tasks which can be matched to specific targets and actions.[4]

Course of Action Support Tool (COAST): The Course of Action Support Tool supports the development, analysis and comparison of candidate Courses of Action (COA) against opposition activities at multiple levels. At the strategic

---

[3] General Dynamics Advanced Information Systems. *Information Warfare Planning Capability*. Online brochure. Arlington, VA: 2007. URL:<http://www.gd-ais.com>. Accessed May 24, 2007.

[4] Ibid.

level, planners are able to use COAST during the Joint Air Estimate Process to develop COAs to support the Component Commander's portion of a theater campaign. COAST also has the ability to develop, analyze and compare multiple friendly COAs and COA variants against most likely and most dangerous adversary COAs, providing strategy planners with options to achieve desired effects. COAST also has branch and sequel capabilities that enable planners to incorporate anticipated changes in the battlespace and respond appropriately. COAST also offers planners the capability to evaluate multiple kinetic and non-kinetic employment options to achieve direct effects. These options can be compared by examining the expected measures of effectiveness achieved by applying the selected capabilities within the context of specific rules of engagement and employment considerations.[5]

Enhanced Synchronization Matrix (eSync): In order to achieve greater efficiency in the conduct of operations, they must be properly synchronized. In addition to planned actions, the effects and evidence of those effects must also be planned and synchronized to facilitate operations assessment. To support synchronization and de-confliction, the Enhanced Synchronization Matrix (eSync) focuses on task and target planned execution timing and desired effect delays and durations. eSync illustrates potential conflicts thus allowing planners to better synchronize kinetic and non-kinetic operations. Further, eSync displays both a timeline of all plan objectives, effects, tasks and targets as well as the desired effect and collection opportunities for each. This feature enhances the planner's ability to satisfy measures of effectiveness in a timely manner by leveraging multiple intelligence sources.[6]

Execution Monitoring Tool (EMT): The EMT displays planned COA elements over time, including COA branch information and selected vs. unselected

---

[5] General Dynamics Advanced Information Systems. *Information Warfare Planning Capability*. Online brochure. Arlington, VA: 2007. URL:<http://www.gd-ais.com>. Accessed May 24, 2007.

[6] Ibid.

elements. Once execution begins, the planner can visualize the entire COA and remain aware of when decision points are drawing near. As decision points are reached, EMT can be used to adjust the decision point criteria and select alternate COA branches if necessary. EMT's Decision Point Map can display upcoming branches and associated decision points, allowing planners to determine whether conditions are being met.[7]

Enhanced Visualization Tool (eViz): The eViz tool supports the geospatial visualization of targets from an IWPC plan or target list. Its features are designed to synchronize and deconflict the multiple capabilities offered by both kinetic and non-kinetic options. To illustrate, eViz highlights duplicate or conflicting targets on a map so users can identify situations where a location is being targeted multiple times or by multiple means. It provides filters to constrain the set of displayed targets based on attributes such as type of action, target source, and desired effect. eViz further supports visualizations of targets, including an organizational view of the relationship between selected facility and unit targets. An understanding of these relationships allows planners and targeteers to leverage capabilities offered by information operations when kinetic means are not desirable or available.[8]

Enhanced Combat Assessment Tool (eCAT): The eCat provides planners and operations assessors with a capability to identify and subsequently assess observable effect and performance indicators as they relate to desired effects. The tool displays the relationships between lower-level direct and indirect effects, as well as their relationship to higher-level effects. Its features multipoint displays that communicate each effect's overall contribution to the campaign, as well as the successes and/or failures of the individually weighted indicators within each effect object. It also displays the cumulative weighted score of individual

---

[7] General Dynamics Advanced Information Systems. *Information Warfare Planning Capability*. Online brochure. Arlington, VA: 2007. URL:<http://www.gd-ais.com>. Accessed May 24, 2007.

[8] Ibid.

effect and performance indicators, and mathematically calculates the performance indicators from the tactical level to higher levels within the plan.[9]

Extensible Markup Language (XML) Briefing Composer (XBC): XBC allows users to generate Microsoft Office products from IWPC XML plan data. This feature enables the generation of documents and briefings either by using supplied IWPC product templates or through creation of a new template. Once generated, the queries and resultant templates may be shared via XBC's Briefing Composer Services.[10]

TEL-SCOPE: The TEL-SCOPE telecommunications modeling and simulation tool supports the target development process as well as critical nodes analysis in support of Intelligence Preparation of the Battlespace. TEL-SCOPE is used to model adversary telecommunications networks and simulate potential targeting scenarios. Using TEL-SCOPE, the operator can display optimal communications paths between selected end-users and then select network nodes or links for disruption, degradation or destruction. TEL-SCOPE can then predict alternate routing for communication traffic within the displayed network. This allows the command and control analyst or targeteer to easily identify potential targets and better predict mission effectiveness. The objective is to select an appropriate set of critical links and nodes that if targeted will achieve the desired effect on the chosen communications paths.[11]

Analyst Collaborative Environment (ACE): To support knowledge management and situational awareness, the ACE enables users to access and share multi-source intelligence and planning information. It provides intelligent search functions and the ability to sort, store and share information between team

---

[9] General Dynamics Advanced Information Systems. *Information Warfare Planning Capability.* Online brochure. Arlington, VA: 2007. URL:<http://www.gd-ais.com>. Accessed May 24, 2007.

[10] Ibid.

[11] Ibid.

members. For message query and retrieval, ACE leverages a multi-source database allowing operators to query intelligence documents ranging from daily mission reports and battle damage assessments to planning documents.[12]

Interactive Scenario Builder (Builder): Builder is a simulation tool that provides insight into and visualization of platforms' radio frequency (RF) capabilities and provides geospatial and temporal situation awareness. Builder models communication and radar systems by calculating one-way and two-way RF propagation loss. It incorporates antenna pattern data and the effects of meteorology, terrain, environment and countermeasures when computing propagation values.[13]

Target Prioritization Tool (TPT): The TPT is used to analyze the space and terrestrial network, providing situational awareness through Intelligence Preparation of the Battlefield and Predictive Battlespace Awareness. TPT then provides a prioritized target list using the commander's objectives set forth in the air campaign plan. Users construct scenarios to achieve desired effects against an adversary network and analyze the network for possible limitations. The analyst can then build possible targeting schemes based on the objectives currently under consideration and the desired effects based on current or future rules of engagement.

Collaborative Workflow Tool (CWT): The Collaborative Workflow Tool (CWT) provides the capability to track workflow progress across distributed teams by providing common checklists that are accessed by team members. Planners and analysts create "workflow templates" that define a standard set of procedures to follow when performing common tasks or processes. Each template may be saved and a workflow created from previous templates and

---

[12] General Dynamics Advanced Information Systems. *Information Warfare Planning Capability.* Online brochure. Arlington, VA: 2007. URL:<http://www.gd-ais.com>. Accessed May 24, 2007.

[13] Ibid.

common checklists. Using a workflow, the operator can track the progress and status of each step and initiate the application or access data source required to accomplish a step.[14]

Information Operations Navigator (ION): The Information Operations Navigator provides users with a standardized, structured methodology for generating IO portions of operations plans in a Joint Operational Planning and Execution System format. ION uses a strategy-to-task methodology to derive IO objectives from overall combat commander objectives and is structured to take the planner through the Joint Information Warfare Operations Command's Joint Information Operations planning process. The user identifies the effects IO must induce on an adversary to accomplish the objectives, and then uses this information to write the corresponding IO tasks.[15]

Collectively, IWPC represents a step forward in terms of harnessing automation and collaboration in order to plan and execute more efficient IO. However, despite the capabilities this suite of applications offers, it cannot be considered as fully representative of IO. The following section examines the limitations of IWPC in the context of what is required for a holistic consideration of IO.

C.   LIMITATIONS

To preface this discussion, it should be understood that IWPC represents a significant improvement in the use of automation to support IO. Contrasted against the myriad tools used in previous generations, it incorporates numerous tools that are highly applicable to the improved conduct of IO and facilitates a degree of collaboration previously unseen. Its limitations stem primarily from being a single service initiative, adopting a "horizontal" approach in the suites various applications, and a critical dependency on collaboration and reachback to gain system knowledge.

---

[14] General Dynamics Advanced Information Systems. *Information Warfare Planning Capability.* Online brochure. Arlington, VA: 2007. URL:<http://www.gd-ais.com>. Accessed May 24, 2007..

[15] Ibid.

As a single service initiative, IWPC rightfully reflects the capabilities resident within the service in which it was developed, in this case, the United States Air Force. This has resulted in a much greater emphasis on applications supporting competencies in IO as practiced by the Air Force rather than IO as practiced by other services. What is noticeably absent, however, is a holistic view of all activities that comprise IO. This significantly reduces the potential applicability of the application when one considers the range of capabilities present in both other services and agencies.

As previously stated, IWPC also incorporates several "horizontal" applications. These applications work well in terms of being readily adapted to various disciplines, but this characteristic also reduces them to what is essentially mission planning software with strong visualization tools. Absent either explicit or tacit knowledge of the respective sub-disciplines, the applications are limited in scope in terms of reasoning capacity which in turn limits the degree of automation that can occur. To progress towards embedded, tacit knowledge a stronger emphasis needs to be placed on depth within the sub-disciplines nested under a more expansive reasoning framework. The use of ontologies provides a means to accomplish this.

As a final consideration on the perceived limitations of IWPC, the emphasis on collaborative tools frame the system in such a manner that it effectively reduces the impetus to better capture tacit knowledge. In this regard, the system relies on human to human exchange to facilitate the spread of knowledge through a conduit made possible by IWPC and a transmission medium. The frailty of this is that the system becomes limited by the human element. Among others, disparities in individual knowledge levels, personnel turnover, and illness each create a degree of variation in the effectiveness of the system. The emphasis on collaboration precludes the capture of tacit knowledge within the automated portion of the system and thus limits the depth of machine to machine exchanges. While collaboration is an essential component of all military operations, developing dependencies on a human knowledge base that may not be accessible introduces a significant limitation.

D.   THE SEMANTIC ADVANTAGE

Based on the preceding discussion of limitations, the intuitive question then becomes how to go about correcting them. The intuitive answer is to extend the scope of the disciplines encompassed by an IO application, add depth to each, and aggregate them under a reasoning framework that facilitates some degree of automated interpretation. Each of these elements can be addressed to some degree through the use of the semantic web and semantic web applications. The IO domain is one of continually expanding capabilities. As a result, supporting software must be adaptive to new circumstance. The Semantic Web has the potential to support this.

By design, the semantic web can quickly incorporate new concepts. Conceptually the semantic web consists of a layered pyramid as depicted in Figure (1).[16] Prior to the semantic web, semantics had to be hard-coded into software or database schemas. While this lends itself well to specific applications, it does not lend itself well to common representation through differing applications or domains. The semantic web allows for the explicit definition of a domain using a common representation thereby reducing ambiguity and thus increasing interoperability.[17] Ontologies are "layered" on top of the RDF subsequently adding greater depth to the vocabulary for describing properties and classes, relations between, cardinality, equality, richer typing of properties, characteristics of properties and enumerated classes.[18] These fundamental aspects of semantic design lend themselves to the kind of adaptability required to support an evolving, adaptable IO application.

---

[16] S. Chance and M. Hagenston. *Assessing the Potential Value of Semantic WebTechnologies in Support of Military Operations*. Monterey, CA: NPS, 2003.

[17] L. Lacy. *OWL: Representing Information Using the Web Ontology Language*. Canada: Trafford.
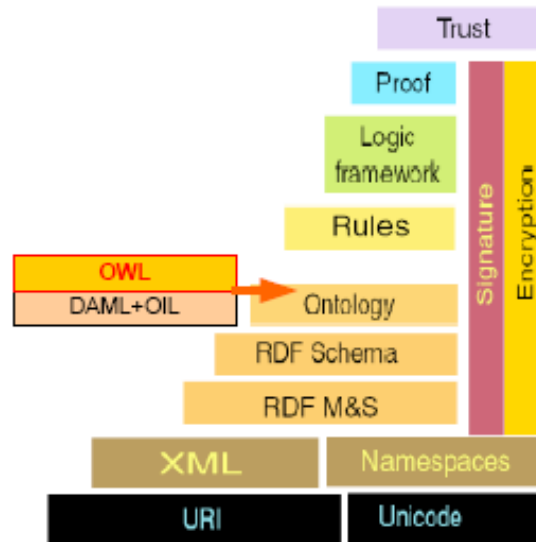
[18] Ibid.

Figure 1.   Semantic Pyramid. (From: 16)

Accepting that the basic design of the Semantic Web lends itself to adaptability, the challenge of "depth within discipline" remains unanswered.   Each of the IO disciplines are predicated on continuously accruing data ranging from imagery, to signal intercepts, to personality profiles. A reasoning framework absent the information to reason about is of decidedly limited utility. For that reason, it will be necessary to make existing database content available for emerging Semantic Web applications.[19]   This challenge has been addressed by researchers at the University of Oregon and Yale University who have used Semantic Web ontologies to incorporate database schemas.

As databases are defined by schemas, the research team was able to develop an automatic translator to represent schemas as ontologies, implying that the task may be able to be automated.[20] This lends itself to evolving semantic web applications that can be expanded to accommodate a changing environment while also drawing from discipline specific data repositories. The combination of adaptability and depth offer a means by

---

[19] Dejing Dou, et al. "Integrating Databases into the Semantic Web through an Ontology-based Framework" Proceedings of the 22nd International Conference on Data Engineering Workshops, 2006.

[20] Ibid.

which the knowledge base of a discipline can be incorporated in the context of multiple reasoning ontologies, facilitating a higher degree of cross discipline synergy within the IO problem domain.

The final points for consideration are the degree and type of collaboration that the semantic web enables. A reliance on a human knowledge base imposes the limitations of humanity. While this is not meant to imply that human to human collaboration should not occur, the ability for machines to exchange and understand information sets conditions for greater automation. This allows humans to defer lower level tasks to the machines while focusing human energy on more complex challenges. The capability for machines to exchange and understand data is fundamental to the Semantic Web.[21] It stands to reason that these benefits can readily be extended into the IO domain.

The web as it currently exists is intended for humans to display, look up and interpret data. As a result, it is structured to present information in a human-friendly manner.[22] While web languages provide a means for structuring data in a human-readable form, they do not provide any explicit meaning that can be read and used by machines. Berners-Lee's vision of the semantic web is to provide an extension to the web as it currently exists to one where data is given additional meaning through its structure. The relationships between data become more explicit as metadata is added to already existing data, creating machine-interpretable content.[23] Systems are expected to use this data to perform tasks that currently require human intervention.[24]

E.   CONCLUSIONS

Collectively, IO has gained increasing recognition as a vital strategic resource.[25] This has lent itself to an understanding that by using a variety of different capabilities and sequencing them appropriately, the face of conflict can be dramatically altered. IWPC

---

[21] Berners-Lee, Tim. (1999). *Weaving the Web*. New York: HarperCollins Publishers, Inc.

[22] Ibid.

[23] Ibid.

[24] C. Childers, *Applying Semantic Web Concepts to Support Net-Centric Warfare Using the Tactical Assessment Markup Language (TAML).* Monterey, CA: NPS, 2006.

[25] Joint Chiefs of Staff. Joint Publication 3-13. *Information Operations.* Washington, DC: GPO, 13 February 2006.

represents a significant step forward in that it considers IO more broadly than any earlier applications. Despite the progress that it represents, it also has limitations. As a single-service initiative, IWPC primarily reflects the competencies of one service. The suite of applications is sufficiently broad to accommodate multiple disciplines, but in achieving this breadth, depth is sacrificed. Finally, there is a critical dependency on human collaboration as a means of exchanging knowledge. This mechanism fails to imbed knowledge within the system, and in doing so creates an external dependency. The semantic web is developing along multiple fronts that have the potential to mitigate these shortcomings.

IV. DEFINING THE DOMAIN

For a strong adversary (corps) the opposition of twenty-four squadrons and twelve guns ought not to have appeared very serious, but in war the psychological factors are often decisive. An adversary who feels inferior is in reality so.

Field Marshal Carl Gustav Baron von Mannerheim
The Memoirs of Field Marshal Mannerheim, 1953

A. THE INFORMATION OPERATIONS PROBLEM DOMAIN

Developing applications that support Information Operations (IO) presents a significant challenge in that the depth and breadth of IO spans multiple and diverse disciplines with a desired end state that encompasses effects well beyond the traditional, physical realm. Further, each of the core, related, and supporting disciplines constitute distinct bodies of knowledge in their own right that cumulatively span multiple services, departments, agencies, and classifications. While an all inclusive IO application would, as a matter of necessity, encompass each of these characteristics this exceeds the scope of this thesis. The focus of this chapter is to define the elements of the IO problem domain that will be further developed in the forthcoming ontology.

While the basis of this chapter will be grounded in joint doctrine, the ontology will be extended as required to encompass additional capabilities discussed in other IO literature and disciplines that will be included in the ontology will be discussed in greater detail. Further, the information contained in this chapter will be presented in a generally hierarchical fashion whereas the ontology will employ differing levels of abstraction and aggregation to facilitate the ease of future expansion. The primary intent of the ontology is to reflect an approach towards developing IO applications for the semantic web as opposed to fully developing said application.

B. IO PRIMER

At the highest level, IO consists of three broad categories; core, supporting, and related capabilities. Each of these categories contains several other disciplines. Core capabilities consist of Psychological Operations, Military Deception, Operations

Security, Electronic Warfare, and Computer Network Operations. Supporting capabilities consist of information assurance (IA), physical security, physical attack, counterintelligence, and combat camera. Related capabilities consist of public affairs (PA), civil military operations (CMO), and defense support to public diplomacy. These capabilities are summarized in Figure (2). For the purpose of this thesis, discussion will be limited to specific elements within the core capabilities.[26]

CORE CAPABILITIES	
Electronic Warfare	Military Deception
Computer Network Operations	Psychological Operations
Operations Security	

SUPPORTING CAPABILITIES	RELATED CAPABILITIES
Information Assurance	Public Affairs
Physical Security	Civil-Military Operations
Counterintelligence	Defense Support to Public Diplomacy
Physical Attack	
Combat Camera	

DoD Information Operations: "The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making, while protecting our own."

Figure 2.   IO Capabilities. (From: 26)

Notably, no single service is the sole repository for IO capabilities. As a case in point, although the Marine Corps may assist in the conduct of PSYOPS, it has no designated PSYOPS structure.[27] Further, in instances where multiple services possess a capability, such as Electronic Warfare (EW), the application generally resides within the core competencies of the given service. Air Force EW assets tend to reside on aircraft, whereas the Army and Marine Corps employ several ground based EW systems. As the

[26] U.S. Army War College, Dept. of Military Strategy, Planning, and Operations. *Information Operations Primer: Fundamentals of Information Operations.* Carlisle, PA. 2006.

[27] Joint Chiefs of Staff. Joint Publication 3-53. *Doctrine for Joint Psychological Operations.* Washington, DC: GPO, 5 September 2003.

capabilities are spread throughout the services, as well as other organizations and departments, an ontology framed solely around service capabilities alone would fail to capture the full range of options that are available in joint operations. For this reason, it is generally advantageous to consider IO in broader terms of capability and platform rather than in the context of a single service.

The range of IO capabilities makes available a multitude of potential options. In order to frame this thesis, primary emphasis will be applied to Psychological Operations and Electronic Warfare. These two capability sets present a reasonably disparate composition of methods, platforms, and service disposition which, while accommodating a great deal of diversity, remains well bounded. While this will not yield a holistic IO ontology, these two disciplines are sufficient to illustrate a methodology for characterizing IO capabilities.

C.   PSYCHOLOGICAL OPERATIONS

Prior to crafting the ontology, some level of domain knowledge must be established. The intent of this section is to introduce the fundamental capabilities, platforms, and service affiliations of primary DoD PSYOP capabilities to establish a frame of reference for the ontology. While several references were reviewed in developing this section, the settled knowledge in the domain of PSYOP as practiced by the U.S. DoD was predominantly found in joint doctrine. For this reason, doctrinal publications serve as the basis for discussion. As such, this should not be considered an exhaustive treatment of the discipline. The intent is to provide sufficient domain knowledge to illustrate the proposed ontological methodology. Given the scope of the ontology, these are adequate to develop the domain.

PSYOP, broadly defined, "are planned operations to convey selected information and indicators to foreign audiences to influence the emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals."[28] As such, PSYOP play an integral role in U.S. diplomatic,

---

[28] Joint Chiefs of Staff. Joint Publication 3-53. *Doctrine for Joint Psychological Operations.* Washington, DC: GPO, 5 September 2003.

informational, military, and economic activities. Each of the respective services is capable of providing some degree of support to PSYOPs.

In terms of ground based PSYOP, the U.S. Army maintains the most robust organization and set of capabilities. The Army maintains one Active Component (AC) PSYOP group and two Reserve Component (RC) PSYOP groups. While the AC PSYOP group is capable of conducting limited strategic PSYOP, it is primarily focused on the operational and tactical levels of war. In contrast, the two RC PSYOP groups are tactical units characterized by regional expertise and language competencies achieved as a result of being assigned specific geographic responsibilities.[29]

A Psychological Operations Group (POG) plans, coordinates, and executes PSYOP activities primarily at the operational and tactical levels. It is structured to support conventional and special operations forces deployed worldwide, and can support several Joint Psychological Operations Task Forces (JPOTF) at both the combatant command and the Joint Task Force level. A POG may contain a Research and Analysis Division, a Regional PSYOP Battalion, a Dissemination PSYOP Battalion, Tactical PSYOP Battalion, and a EPW/CI/DC PSYOP Battalion.[30] The following excerpts from Joint Publication 3-53. *Doctrine for Joint Psychological Operations* briefly articulate the functions served by each:

> **Research and Analysis Division:** Civilian analysts are employed to add socio-cultural expertise and institutional continuity to the operational skills possessed by the POG. The analysts have advanced degrees and many have military experience. Their knowledge of foreign cultures and their analytical capabilities are critical to the efforts of the 4th POG.[31]

---

[29] Joint Chiefs of Staff. Joint Publication 3-53. *Doctrine for Joint Psychological Operations.* Washington, DC: GPO, 5 September 2003.

[30] Ibid.

[31] Ibid.

Regional PSYOP Battalion: A Regional PSYOP Battalion provides cultural and linguistic expertise and is capable of providing support to two or more organizations within the combatant command.[32]

Dissemination PSYOP Battalion: Dissemination PSYOP Battalions provide audio, visual, audiovisual materials production, signal support, and media broadcast capabilities to the POG, JPOTF, and other PSYOP units.[33]

Tactical PSYOP Battalion: Tactical PSYOP Battalions provide support to corps level units and below, select special operations and conventional task forces. The TPB's capabilities include dissemination of PSYOP products by loudspeaker message, leaflet, handbill, and face-to-face communications.[34]

EPW/CI/DC PSYOP Battalion: Collects and evaluates PSYOP-relevant intelligence from EPW, Cis, and DCs through interrogations, face-to-face communications, and testing of PSYOP products and themes. Camp functions include dispelling rumors, creating dialogue, and pacifying or indoctrinating EPWs/Cis/DCs to ensure safe and humane conditions.[35]

Taken collectively, the U.S. Army has a diverse set of PSYOP capabilities designed to accommodate operations throughout the Strategic, Operational, and Tactical levels of war. They maintain units that possess geographic focus and others that cultivate competencies in the dissemination of the PSYOP message through multiple means. Additional units add very specific skill necessary to handling the military realities of prisoners and displaced persons. In all, this capability set represents PSYOP through the lens of land warfare.

---

[32] Joint Chiefs of Staff. Joint Publication 3-53. *Doctrine for Joint Psychological Operations.* Washington, DC: GPO, 5 September 2003.

[33] Ibid.

[34] Ibid.

[35] Ibid.

The Army is, of course, not alone in the PSYOP domain. The U.S. Navy also maintains a robust and disparate set of capabilities that support PSYOP initiatives. These capabilities can be generally aggregated under the broad headings of "ashore" and "afloat." The Navy's various shore installations are able to a variety of audiovisual products. Additionally, a reserve unit is maintained to provide audiovisual and training support to USJFCOM.[36]

The Navy's Fleet Information Warfare Center (FIWC), located at the Little Creek Naval Amphibious Base, Norfolk, Virginia, also maintains the ability to provide training in planning and executing PSYOP to assist fleet units. The FIWC is also closely aligned with the Army's 4th POG at Fort Bragg, North Carolina. This facilitates a stronger, shared understanding in terms of PSYOP training, equipment employment, product dissemination, and tactics, techniques, and procedures development in the area of Navy support to PSYOP.[37]

In addition to shore based AV development capabilities, the Navy is developing a high-speed leaflet and handbill production capability for large deck ships. This can be used with naval air assets to rapidly produce and disseminate PSYOP products during the early stages of a crisis. Naval F/A-18 aircraft are able to disperse leaflets by dropping ROCKEYE leaflet bombs. Additionally, most US Navy vessels have the ability to support PSYOP through an organic high frequency transmission capability which can be used to disseminate PSYOP messages through a broadcast medium. Shipborne helicopters are also of utility in PSYOP in that they can support leaflet drops, loudspeaker broadcasts, and humanitarian aid dissemination.[38]

Not unlike the Army, the PSYOP capability set presented by the Navy reflects its composition and specific competencies. Shore installations are used for optimal production and training, whereas assets afloat are used largely in the context of responding to a crisis. The Navy is able to collectively employ its unique blend of ships, planes, and helicopters to support the PSYOP effort.

---

[36] Joint Chiefs of Staff. Joint Publication 3-53. *Doctrine for Joint Psychological Operations.* Washington, DC: GPO, 5 September 2003.

[37] Ibid.

[38] Ibid.

The Air Force also maintains PSYOP capabilities that reflect its service competencies and culture. As would be expected, Air Force contributions to PSYOP focus on applied technology and air and space power, to "prepare, shape, and exploit the psychological dimension of the battlespace."[39] Air Force information warfare flights have individuals located in operations centers that assist commanders in the conduct of IO, to include PSYOP. In this capacity, they coordinate between the operations center and the JPOTF to ensure awareness of an adversary's sociological, cultural, and demographic information and further enable effective PSYOP.[40]

In addition to planning expertise, several Air Force assets have the capability to execute missions in support of PSYOP objectives. To that end, specific aircraft have PSYOP as their primary mission. The EC-130 COMMANDO SOLO aircraft are equipped for airborne broadcasts of PSYOP messages via radio and television signals. Additionally, several airdrop aircraft are capable of performing leaflet airdrop missions, and fighter and bomber aircraft can dispense leaflets by dropping leaflet bombs.[41] Again, the PSYOP capability set presented by the Air Force tends to reflect service strengths.

The Marine Corps is somewhat unique in that it has no organizational PSYOP structure. However, given the nature of the service, it is able to convey audible and visible actions designed to deliver specific messages to an adversary. These may include broadcasts from shore-based or airborne loudspeaker systems and leaflet dissemination by various aircraft. In general terms, PSYOP expertise within the Marine Corps resides in the individual Marines who have received training through joint and service schools.[42]

In examining the service capabilities, several prominent characteristics become apparent. The respective services capabilities tend to match service's primary competencies. As a case in point, the Air Force uses aircraft to broadcast signals while the Navy maintains a similar, shipborne capability. There is also a significant degree of redundancy between services, as both the Navy and the Army maintain a capability to

---

[39] Joint Chiefs of Staff. Joint Publication 3-53. *Doctrine for Joint Psychological Operations.* Washington, DC: GPO, 5 September 2003.

[40] Ibid.

[41] Ibid.

[42] Ibid.

produce large amounts of printed materials. While this redundancy does exist, no single service can fully replicate the capabilities of its sister services, creating a high degree of interdependency to fully saturate a battlespace with a PSYOPS message.

As each service has a PSYOPs capability, there is an implicit need for de-confliction. If two PSYOPS activities are disseminating different messages to the same target audience, the potential effects are largely nullified. Perhaps most relevant to deconstructing the discipline is the mediums employed by all services. Regardless of service and regardless of capability, there is a finite number of means by which the PSYOPS message is disseminated. As depicted in Figure (3), all messages are conveyed by television, radio, newspapers, leaflets, posters, handbills, loudspeakers, or face-to-face communications.[43]
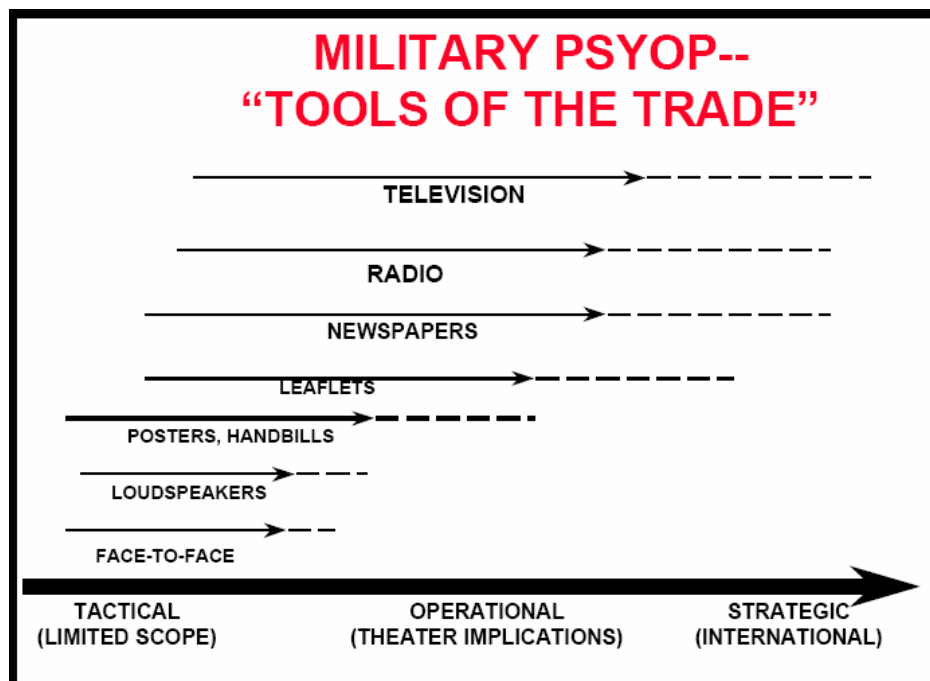

Figure 3.   PSYOP Dissemination Methods. (From: 43)

[43] Office of the Under Secretary of Defense For Acquisition, Technology and Logistics. *The Creation and Dissemination of All Forms of Information in Support of Psychological Operations (PSYOP) in Time of Military Conflict*. Report of the Defense Science Board Task Force. Washington, D.C., May 2000.

By reaching this least common denominator through domain analysis, conditions are now set to begin considering an ontological view of PSYOPS.

D.   ELECTRONIC WARFARE

IO encompasses numerous disciplines. For the purposes of this document, PSYOPS and Electronic Warfare (EW) will be examined. The intent in identifying these two disciplines for examination stems from their reasonably disparate composition of methods, platforms, and service disposition. Not unlike PSYOPS, each branch of the service maintains some type of EW capability, and not surprisingly, the capabilities tend to reflect the service competencies of the owning organization. Further, the settled knowledge in the domain of EW as practiced by the U.S. DoD was predominantly found in joint doctrine, thus doctrinal publications serve as the basis for discussion.

EW is defined as, "Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support."[44] To expand on this, the following definitions of the EW divisions are provided and graphically depicted in Figure (4):

Electronic Attack: Division of electronic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called EA.[45]

---

[44] Joint Chiefs of Staff. Joint Publication 3-13.1. *Electronic Warfare*. Washington, DC: GPO, 25 January 2007.

[45] Ibid.

Electronic Protection: Division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. Also called EP.[46]

Electronic Warfare Support: Division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Also called ES.[47]
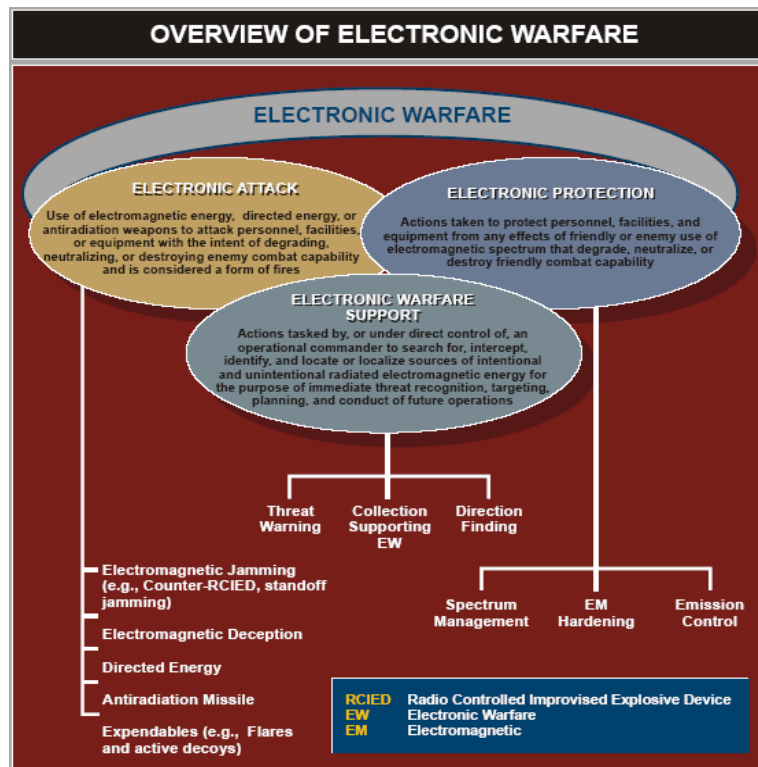

Figure 4.   Overview of Electronic Warfare. (From: 46)

---

[46] Joint Chiefs of Staff. Joint Publication 3-13.1. *Electronic Warfare*. Washington, DC: GPO, 25 January 2007.

[47] Ibid.

Each of the services has adopted EW to help them achieve their respective warfighting functions. In the U.S. Army, EW is focused on disrupting, delaying, diverting, and denying the adversary's ability to wage war while also protecting friendly use of electronics systems. For conventional operations, the Army's view of EW is linked closely to the combined arms structure of adversary forces and the manner in which adversary combatants conduct combat operations. The mobility, speed, range, accuracy, and lethality of opposing forces place an emphasis on the command and control systems of ground force commanders.[48]

The Army seeks to achieve synchronization by integrating EW into both the IO plan and fire support operations to support the ground scheme of maneuver. To achieve this, the Army maintains limited organic air and ground-based EW resources to support operations. As resources are limited, mission requirements tend to exceed operational capability. To mitigate against these shortfalls, EW support from other services is often synchronized with Army combat operations to ensure the success of joint military operations. Given this dependency on external capabilities, joint planning and coordination are critical to synchronizing joint EW.[49]

The U.S. Navy employs EW in surveillance, the neutralization or destruction of adversary targets, and the enhancement of friendly force battle management. Naval battle groups employ a variety of shipboard EW systems, primarily for self protection while naval aviation forces are employ carrier and land-based EA-6B Prowlers to conduct EA, ES, and EP in support of Suppression of Enemy Air Defenses (SEAD) and IO. Collectively, naval forces use EA to "deny, deceive, disrupt, destroy, or exploit the adversary's capability to communicate, monitor, reconnoiter, classify, target, and attack."[50]

The Air Force is also capable of conducting the full range of EW operations. Additionally, Air Force EW supports SEAD and other IO mission areas such as the delivery of PSYOP messages and support MILDEC operations. The underlying intent

---

[48] Joint Chiefs of Staff. Joint Publication 3-13.1. *Electronic Warfare*. Washington, DC: GPO, 25 January 2007.

[49] Ibid.

[50] Ibid.

behind Air Force EW is to "increase aircraft survivability, enhance the effectiveness of military operations, and increase the probability of mission success."[51] Foremost among the Air Forces EW assets is the EC-130H Compass Call, capable of performing C2 systems countermeasures, and supporting air, land, and sea operations. Through the use of effective use of EW, the Air Force seeks to reduce the risk associated with attaining air superiority.[52]

The Marine Corps employs EW as an integral element of maneuver warfare. While similar in practice to the Army, the intent of EW in the Marine Corps is to influence the enemy's decision cycle by disrupting his ability to command and control forces. This enhances friendly capabilities while "shattering the moral, mental, and physical cohesion of the adversary, rendering the adversary incapable of effectively resisting."[53] The Marine Corps maintains EW units in both the command and aviation combat elements of a Marine Air-Ground Task Force (MAGTF). Further, EW units are integrated into concept of operations in order to enhance combined arms capabilities. By integrating aviation and ground EW capabilities, the MAGTF is able to maximize their effects in support of mission objectives.[54]

E.   CONCLUSIONS

This thesis has introduced IO with an emphasis on PSYOPS and Electronic Warfare. Although this relatively short treatment provides little more than a framework from which the problem domain may be considered, it is sufficient to begin framing the ontology in the next chapter. Prior to doing so, however, it is worthwhile to briefly consider the emergent themes found in the PSYOPS and EW joint doctrine.

It quickly becomes apparent that each of the services has their own perspective on how to employ PSYOPS and EW capabilities to their best advantage. Further, this perspective tends to be grounded in their core competencies as we tend to see naval units

---

[51] Joint Chiefs of Staff. Joint Publication 3-13.1. *Electronic Warfare*. Washington, DC: GPO, 25 January 2007.

[52] Ibid.

[53] Ibid.

[54] Ibid.

cultivate seaborne capabilities whereas the Army is decidedly oriented towards land warfare. Given their traditional battlespace roles, this is reasonable to expect. These capabilities also invariably reside on some type of platform, be it an individual soldier or an aircraft, which again tend to be reflective of service character. Taken collectively, these combine to form a broad range of employment options for Joint Force Commanders.

While the diversity in capability is worth mention, what is perhaps more interesting for our purposes is how quickly they can be aggregated. Despite the variety in service capabilities, they can each be expressed as a combination of platform and function(s). To elaborate, consider a ship with a printing press and a direction finding capability. This supports both PSYOPS and the ES division of EA, all under the broader rubric of IO. Given that these capabilities can be expressed as an aggregation of the two basic characteristics of platform and function, a top level reasoning framework for the ontology begins to emerge. The focus of the next chapter will be to define a methodology for expressing IO capabilities in an ontology suitable for use on the semantic web.

THIS PAGE INTENTIONALLY LEFT BLANK

V.   DEVELOPING THE ONTOLOGY

> To understand human decisions and human behavior requires something more than an appreciation of immediate stimuli. It requires, too, a consideration of the totality of forces, material and spiritual, which condition, influence or direct human responses. And because we are dealing with human beings, the forces which helped shape their actions must be recognized as multiple, subtle, and infinitely complex.
>
> David Herlihy
> The History of Feudalism

A.   MAN AND MACHINE

An ontology is ultimately a study in abstraction. It is a means to express elements of the material world in a meaningful fashion. This is made more difficult in that there are multiple ways of expressing reality. An airplane can be considered as a singular entity with specific properties, or an aggregation of wings, fuselage, engine, and propeller, each with their own attributes. As reality can be expressed in several ways, several ontologies could be used to frame the same problem domain. The ontology developed in this chapter is one of many ways to characterize IO, and while grounded in doctrine and current literature, should not be considered as the sole means of expressing the environment.

When examining ontologies, the essence of the challenge is the means by which humans and machines respectively "consider" a given domain. This gap is exacerbated in that the means by which we establish doctrinal concepts are intended for human consumption and therefore do not provide a mechanism to readily convey the essence into a format that is machine usable. The intent behind the ontology is to capture domain knowledge in a reasoning framework that is robust enough to accommodate disparity and changing relationships. In order to develop an ontology that is dynamic enough to accommodate changing circumstance, the ontology must be developed such that the level of abstraction is low enough to remain consistent for use on the machine, but high enough to convey meaning to a human.

Figure (5) is an extract from Joint Publication 3-13. It illustrates the core and supporting capabilities of IO as well as their respective activities and the means by which they are aligned with conventional operations. For a human audience, this presents a reasonably intuitive portrayal of what capabilities are resident within IO, how IO is generally employed, why IO is undertaken, where IO fits in the conventional planning processes, and, broadly, who conducts the various facets of IO.

INFORMATION OPERATIONS INTEGRATION INTO JOINT OPERATIONS (NOTIONAL)

Core, Supporting, Related Information Activities	Activities	Audience/ Target	Objective	Information Quality	Primary Planning/ Integration Process	Who does it?
Electronic Warfare	Electronic Attack	Physical, Informational	Destroy, Disrupt, Delay	Usability	Joint Operation Planning and Execution System (JOPES)/ Targeting Process	Individuals, Governments, Militaries
	Electronic Protection	Physical	Protect the Use of Electro-magnetic Spectrum	Security	JOPES/Defense Planning	Individuals, Businesses, Governments, Militaries
	Electronic Warfare Support	Physical	Identify and Locate Threats	Usability	Joint Intelligence Preparation of the Battlespace(JIPB)/SIGINT Collection	Militaries
Computer Network Operations	Computer Network Attack	Physical, Informational	Destroy, Disrupt, Delay	Security	JIPB/JOPES/Targeting Process	Individuals, Governments, Militaries
	Computer Network Defense	Physical, Informational	Protect Computer Networks	Security	JOPES/J-6 Vulnerability Analysis	Individuals, Businesses, Governments, Militaries
	Computer Network Exploitation	Informational	Gain Information From and About Computers and Computer Networks	Security	JIPB/Targeting Process	Individuals, Governments, Militaries
Psychological Operations	Psychological Operations	Cognitive	Influence	Relevance	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
Military Deception	Military Deception	Cognitive	Mislead	Accuracy	JOPES/Joint Operation Planning	Militaries
Operations Security	Operations Security	Cognitive	Deny	Security	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
Supporting Capabilities	Information Assurance	Informational	Protect Information and Informatin Systems	Security	JOPES/J-6 Vulnerability Analysis	Businesses, Governments, Militaries
	Physical Security	Physical	Secure Information and Information Infrastructure	Usability	JOPES/Defense Planning	Businesses, Governments, Militaries
	Physical Attack	Physical	Destroy, Disrupt	Usability	JOPES/Joint Operation Planning	Governments, Militaries
	Counterintelligence	Cognitive	Mislead	Accuracy	JIPB/Human Intelligence Collection	Governments, Militaries
	Combat Camera	Physical	Inform/Document	Usability, Accuracy	JOPES/Joint Operation Planning	Governments, Militaries
Related Capabilities	Civil Military Operations	Cognitive	Influence	Accuracy	JOPES/Joint Operation Planning	Governments, Militaries
	Public Affairs	Cognitive	Inform	Accuracy	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
	Public Diplomacy	Cognitive	Inform	Accuracy	Interagency Coordination	Governments

Figure 5.   IO Integration. (From: 25)

Even absent further information, humans can reason about what is resident in this table and begin to conceive operations that sequence and combine the capabilities in such a manner that the possibility of greater operational synergy begins to emerge. Military Deception in concert with Information Assurance and Electronic Protection masks intent from an adversary. Electronic Attack coupled with Computer Network Attack and Psychological Operations precludes effective enemy communication and affords an opportunity to send a message of the IO practitioners choosing. Succinctly, humans with

a basic understanding of IO capabilities can infer a multitude of possibilities from this single figure, a machine cannot. The ontological challenge is to present these capabilities in a manner understandable by both.

B.   INFORMATION OPERATIONS DOMAIN CONCEPT

Having examined IO capabilities in the preceding chapters, the issue becomes one of expression at a level of aggregation high enough to encompass all possible entities while still conveying key discriminators. To frame this in our problem domain, we can express Information Operations Resources as an aggregation of platforms and capabilities (Figure (6)). Note that this framework requires a broad interpretation of platform, insomuch as this could be a PSYOPS soldier or an aircraft. In the case of the former, his relationship with capability may be face-to-face dissemination of the PSYOPS message. In the case of the latter, it may be a jamming capability resident on the aircraft.

Expressed in these terms, two significant benefits quickly become apparent. The human can intuitively grasp the concept of platform and capability. For the machine, this defines a top-level set of relationships with logical rules that can be adhered to. Information Operations Resources must be considered in terms of platforms and capabilities. Each platform must have an IO capability to fit into this framework, and each capability must reside on a platform. This small set of logical rules can be captured in the Protégé tool and be extended to accurately express IO assets.
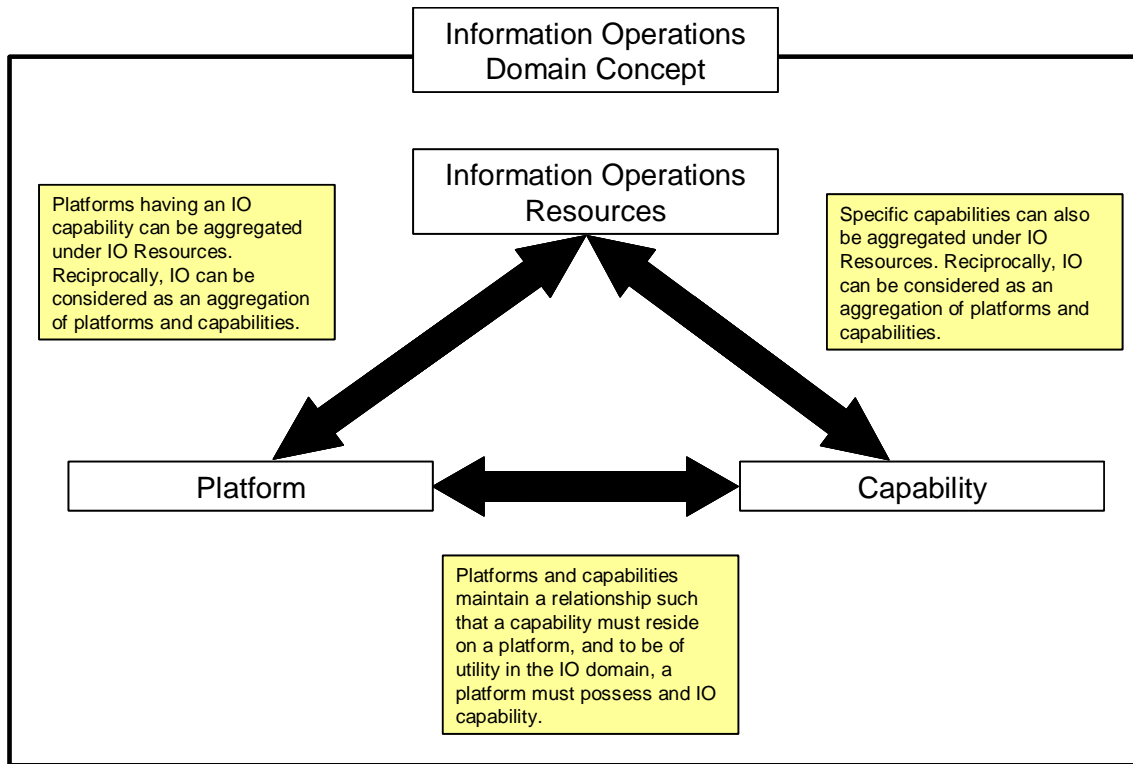
Figure 6.   IO Domain Concept.

While the governing rules established in the preceding paragraph are adequate to broadly characterize the problem domain, additional fidelity is required to enable further reasoning. The next ontological echelon provides another logical layer to enrich the machines capacity to reason about the domain. To achieve this, the aggregations of platform and capability are expanded with additional subsets and logical rules (Figure (7)). The aggregation of platform must consist of at least one of the subsets of air, land, sea, or space. Regardless of the platform in question, it has to reside in one or more of these physical mediums. For the purposes of this thesis, capabilities will be further expanded to encompass the core IO capabilities of Electronic Warfare, Computer Network Operations, Psychological Operations, Operations Security, and Military Deception. Supporting and related capabilities are intentionally excluded, but could easily be incorporated within this framework.
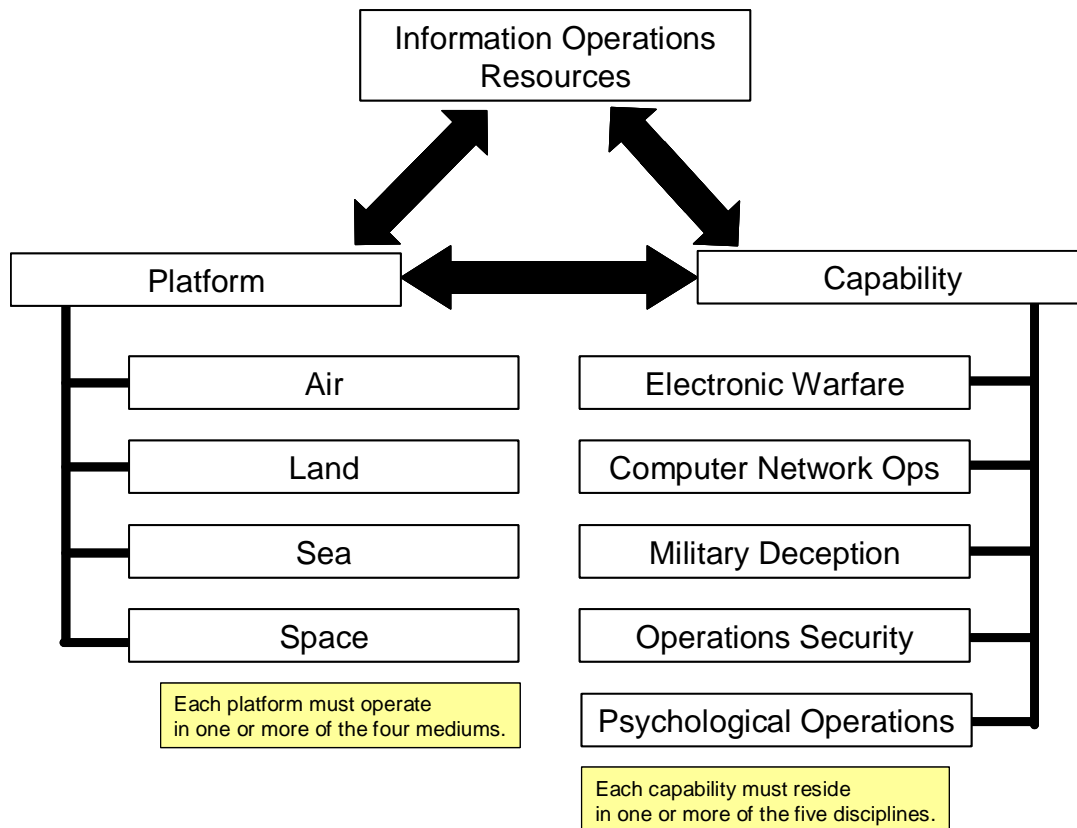
Figure 7.   Aggregation of IO Resources.

Having established the basic rules for defining IO, conditions are set to begin populating the ontology with more concrete assets. In the following example, specific platforms and capabilities are established under air and land platforms and electronic warfare and psychological operations capabilities (Figure (8)). In this instance, Tactical PSYOP Battalion is placed under platform and leaflet dissemination is placed under capability. Similarly, the EA-6B is placed under the heading of air platform while its jamming system, the USQ-113(v)3 is placed under capabilities. While it may seem counterintuitive to disaggregate elements of the airframe, this is a critical element of the reasoning framework. As the USQ-113 may also be used on other platforms, this allows for the expansion of the jammer's associations.[55]

---

[55] Jane's Intelligence Centres. << http://www8.janes.com.libproxy.nps.edu/Search/documentView.do? docId=/content1/janesdata/yb/jav/jav_1299.htm@current&pageSelected=allJanes&keyword=tank&backPath=http://search.janes.com/Search&Prod_Name=JAV&keyword= >>. Accessed 26 March 2008.

In this instance, EA-6B and Tactical PSYOP Battalion are placed under their respective platform headings. The USQ-113(v)3 jammer and leaflet dissemination are categorized appropriately under capabilities. The relationships are defined in the rules set in the Protégé ontology editor.
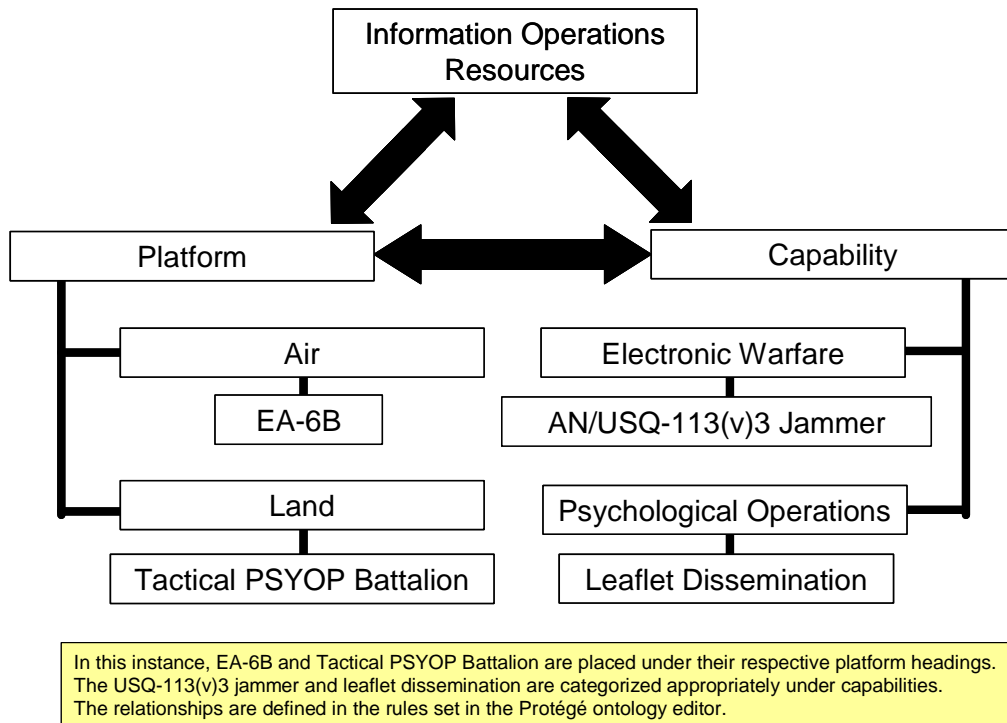
Figure 8.   Expansion of IO Resources.

From an ontological standpoint, the reasoning framework is established. The next step is to populate it in a tool that supports its use on the Semantic Web. To achieve this, Stanford's Protégé tool will be employed. Protégé allows the user to define the rules and relationships of the domain and export the file in an RDF or OWL format which supports its use on the Semantic Web. The following screen captures illustrate how the reasoning framework was captured in Protégé. OWL Source code is contained in Appendix A.
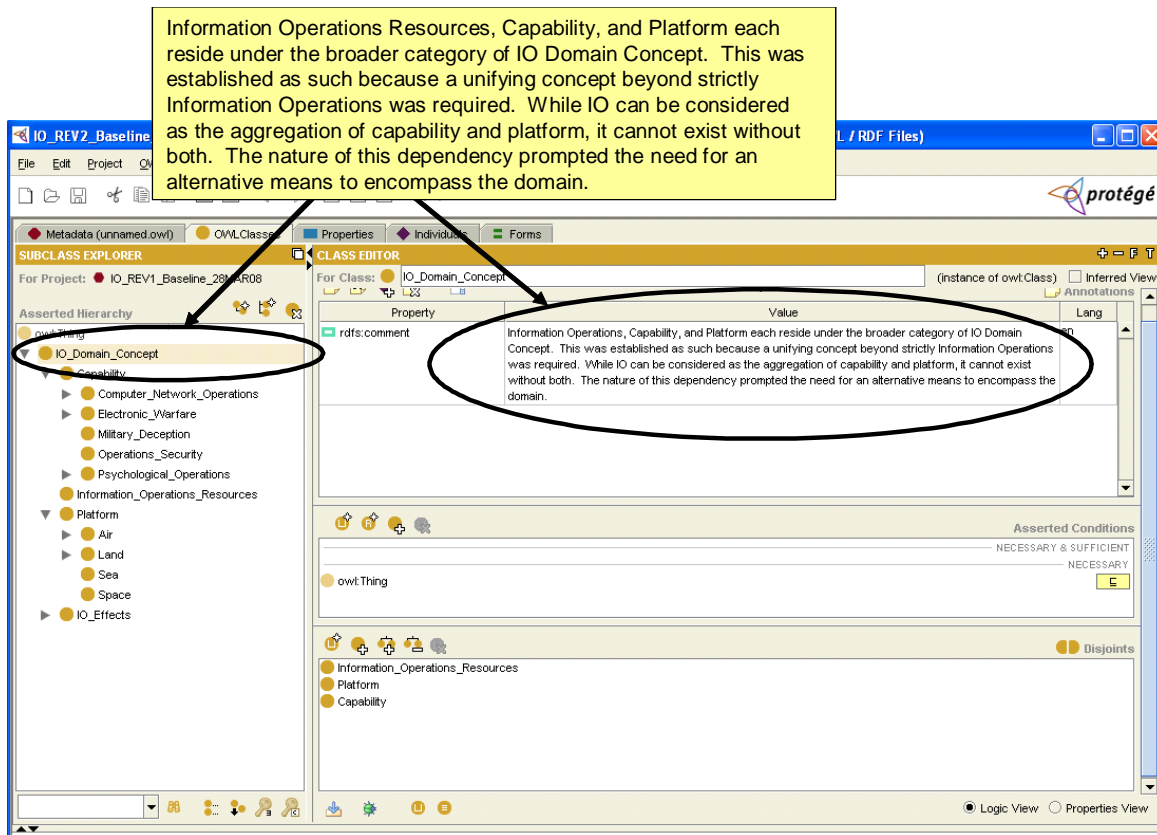
Figure 9.   IO Hierarchy in Protégé.

The preceding figure illustrates the introduction of the IO Domain Concept. While IO aggregates capabilities and platforms, it is not a purely hierarchical relationship. For IO to be undertaken, it must have a capability and a platform. Absent either of these entities, nothing can occur. Expressed differently, the presence of a platform does not of itself enable anything unless a capability resides on it. A capability absent a platform is similarly limited. As structured in Protégé, IO Domain Concept allows Information Operations, Platforms, and Capabilities to be considered with a parity that reflects operational reality. The following figure reflects how this relationship is defined.
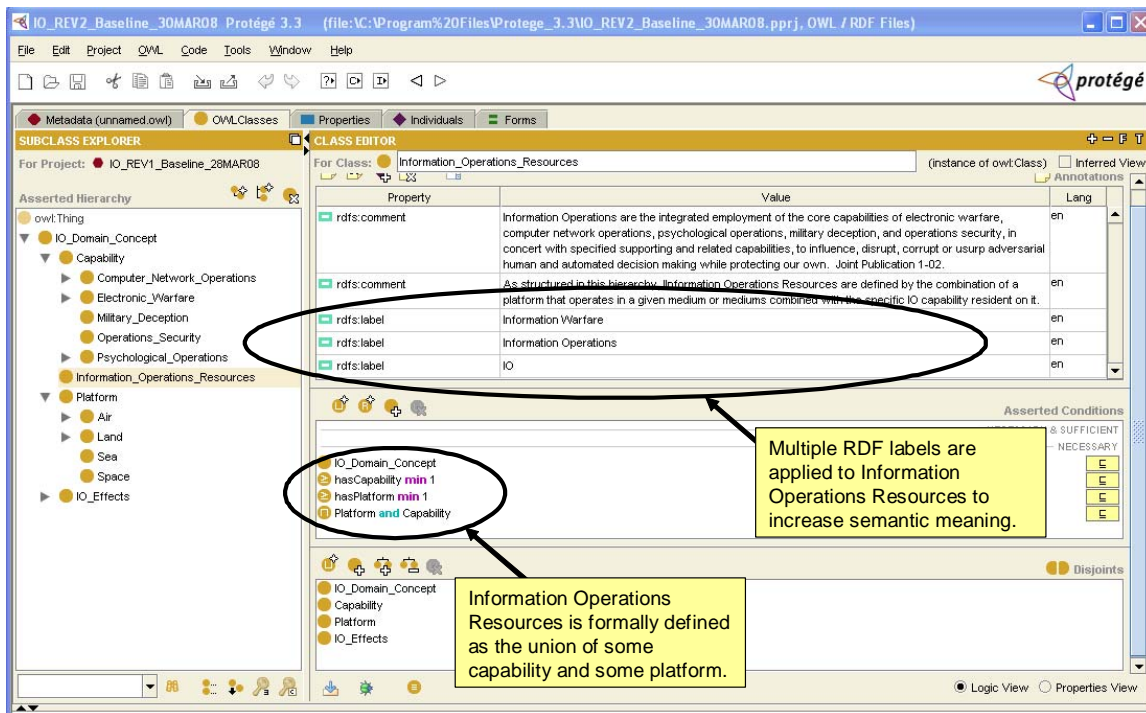
Figure 10.   Domain Rules in Protégé.

Figure (10) illustrates two fundamental elements underpinning the Semantic Web. The first is that the class Information Operations Resources is assigned multiple RDF labels to enable an increased ease of location. The second is that the relationship between IO is semi-formally defined as consisting of some elements of Capability and some Elements of Platform. The use of these rules provides a means by which machines can better reason about the problem domain. As will become evident, similar rules are applied to define the relationship of other classes and subclasses throughout the domain. The following figures illustrate this in the context of the example previously introduced in this chapter.
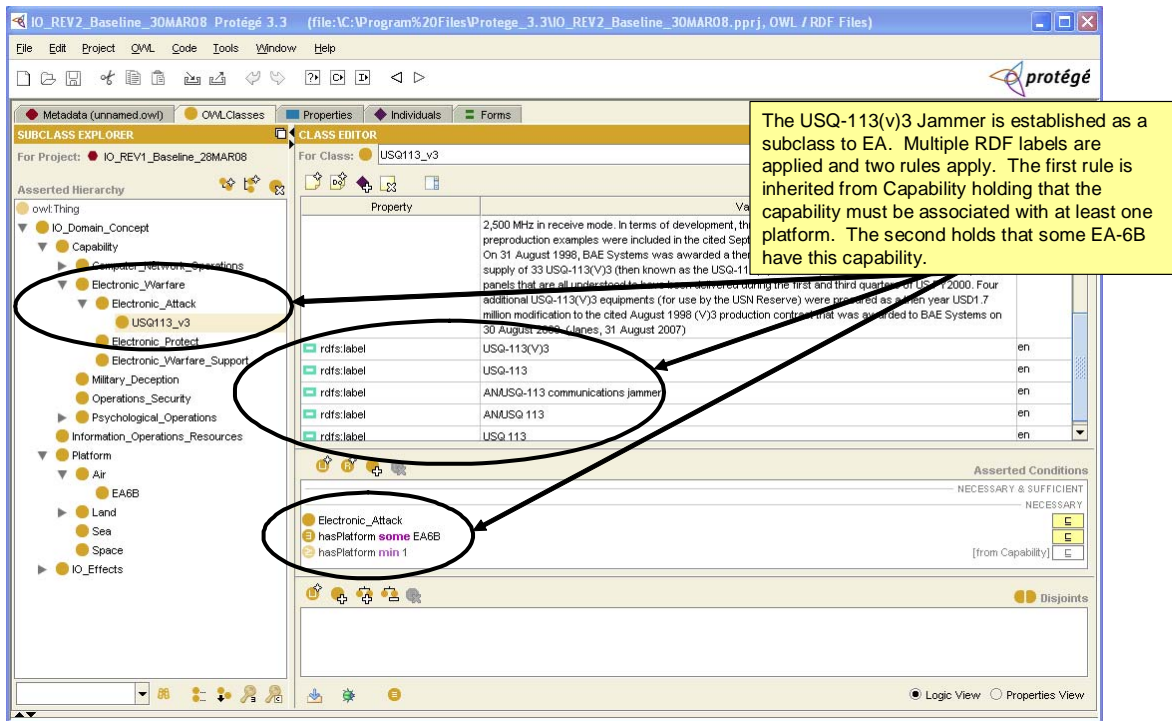
Figure 11.   USQ-113(V) 3 Concrete Class in Protégé.

Figure (11) illustrates the means by which concrete classes are addressed in the ontology.   In this instance, the USQ-113(V) 3 jammer is identified as a concrete class residing under the Electronic Attack and Electronic Warfare.   Multiple semantic labels are affixed to it and rules are established to ensure that it is associated with at least one platform, some of which are the EA-6B.   Of note, the rule requiring an association with a minimum of (1) platform is inherited from the superclass, Capability.   This rule is universally applied to all subclasses residing under Capability.   As will be seen in the following figure, the EA-6B platform has a complementary set of rules that define its relationship with the USQ-113 (V) 3 jammer.
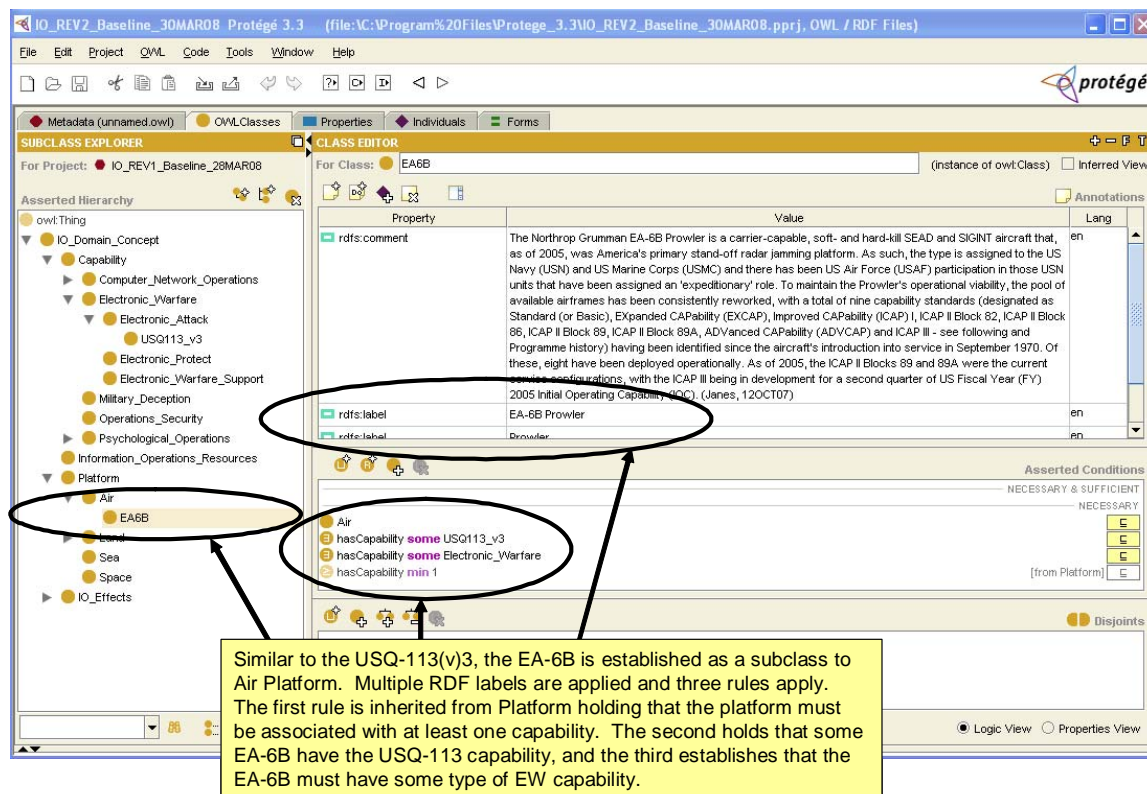
Figure 12.   EA-6B Rule Set in Protégé.

To complete the example, Figures (13) and (14) illustrate how this is applied to the PSYOP capabilities and platforms previously introduced. While the content differs to reflect the specific characteristics of the IO Resource, the methodology for characterization remains constant. The only noteworthy distinction is the number of RDF labels affixed to Leaflet Dissemination.
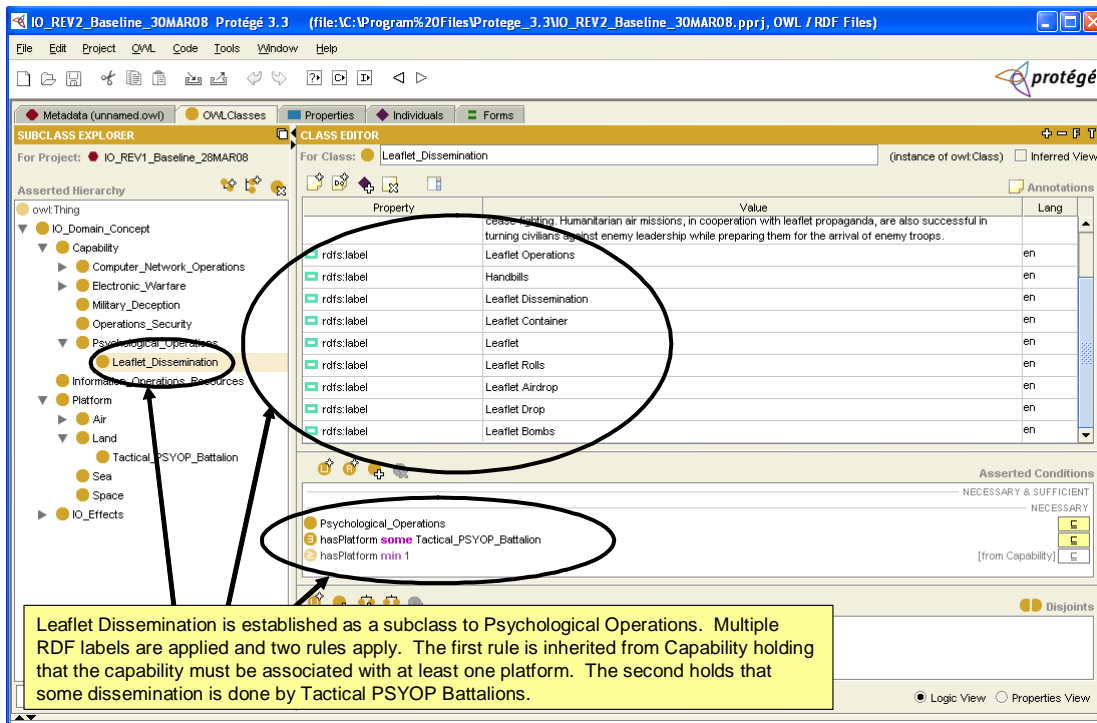
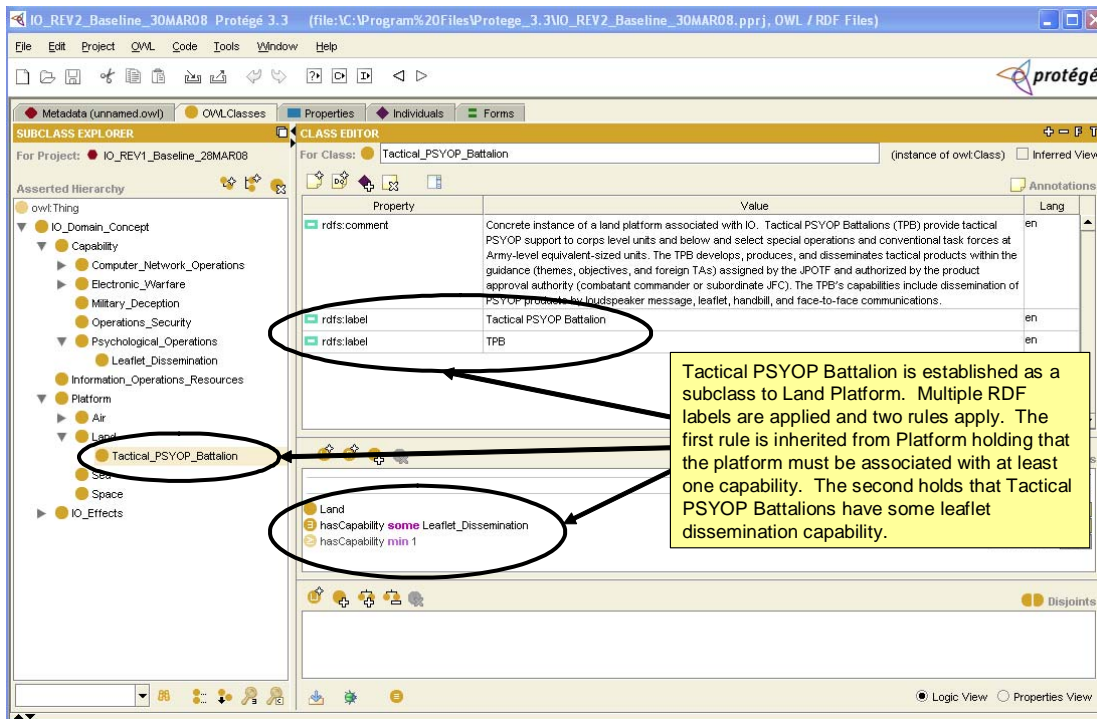Figure 13.   Leaflet Dissemination Rule Set in Protégé.

Figure 14.   Tactical PSYOP Battalion Rule Set in Protégé.

C.   EXPANDING THE DOMAIN

What has been provided to this point is a means of reasoning about how the combination of Platforms and Capabilities equates to an Information Operations Resource. Intuitively, the next step should give consideration to how these resources are applied and what effects they may have. To achieve this, the Information Operations Domain Concept needs to be expanded to address IO effects, as illustrated in Figure (15).
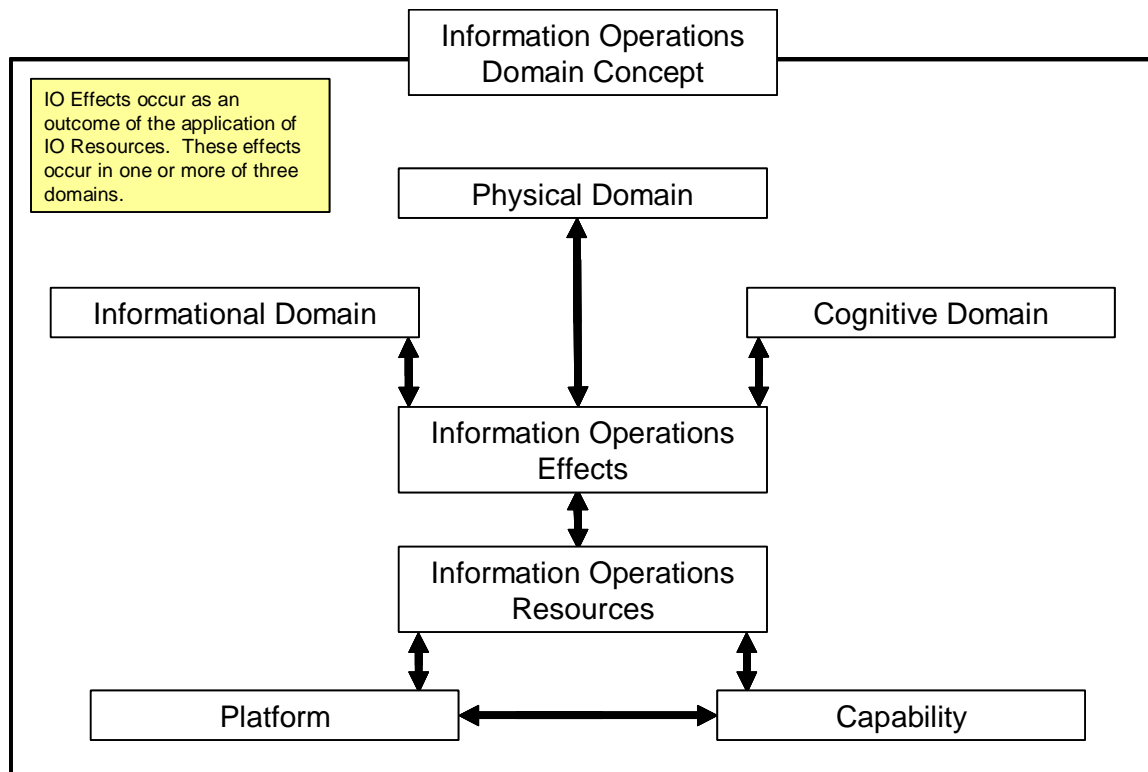

Figure 15.   Expansion of the IO Domain Concept.

The preceding figure builds upon the initial concept of Information Operations Resources and expands it to incorporate Information Operations Effects. These effects are achieved in any combination of the Informational, Physical, or Cognitive domains. By expanding the content of the overarching IO Domain Concept, it is now possible to

begin defining the relationships between the application of a specific IO Resource and the effects associated with it. The following figures illustrate how these relationships may be defined in the Protégé tool.
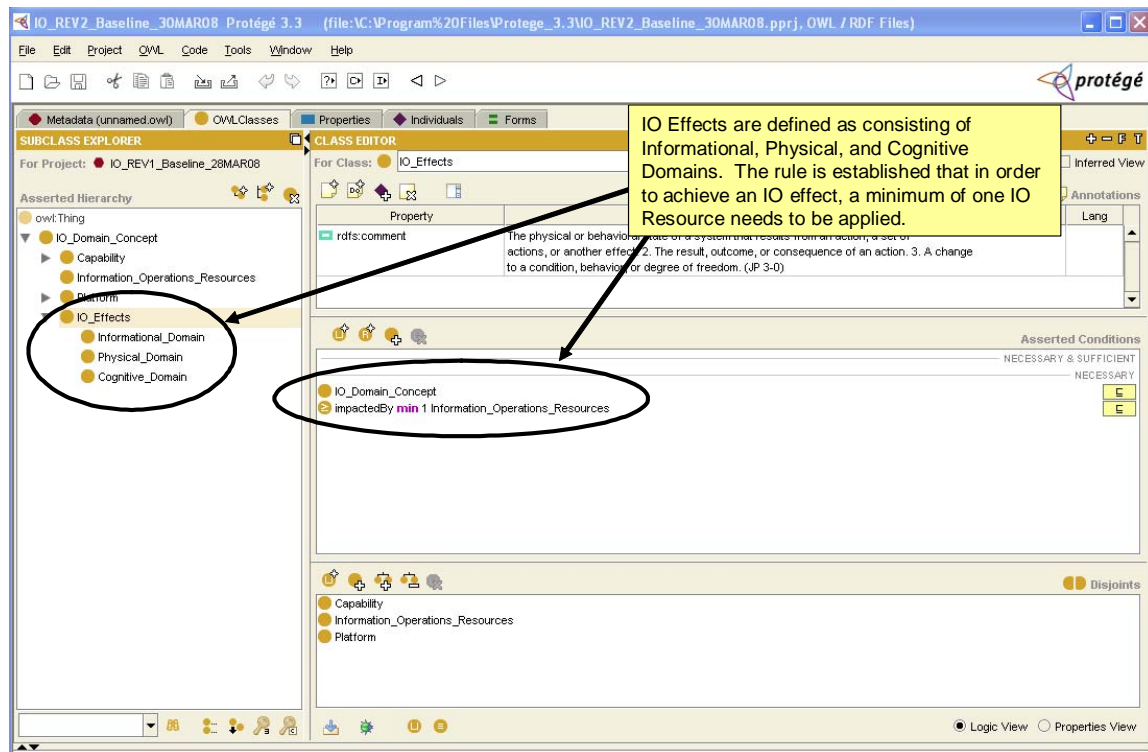

Figure 16.   Expansion of IO Domain Concept in Protégé.

Figure (16) illustrates that the original IO Domain Concept is expanded to include the new superclass of IO Effects, consisting of the subclasses of Informational Domain, Physical Domain, and Cognitive Domain. A rule is established such that in order to achieve an IO Effect, one or more IO Resources need to be applied. The specific subclasses of IO Effect establish the nature of the relationship between the effect and the resource applied. As an example, in Figure (17) a rule is established to assert that the Cognitive Domain is impacted by the presence of Psychological Operations. As the IO Domain Concept becomes more fully developed, additional rules would need to be added.
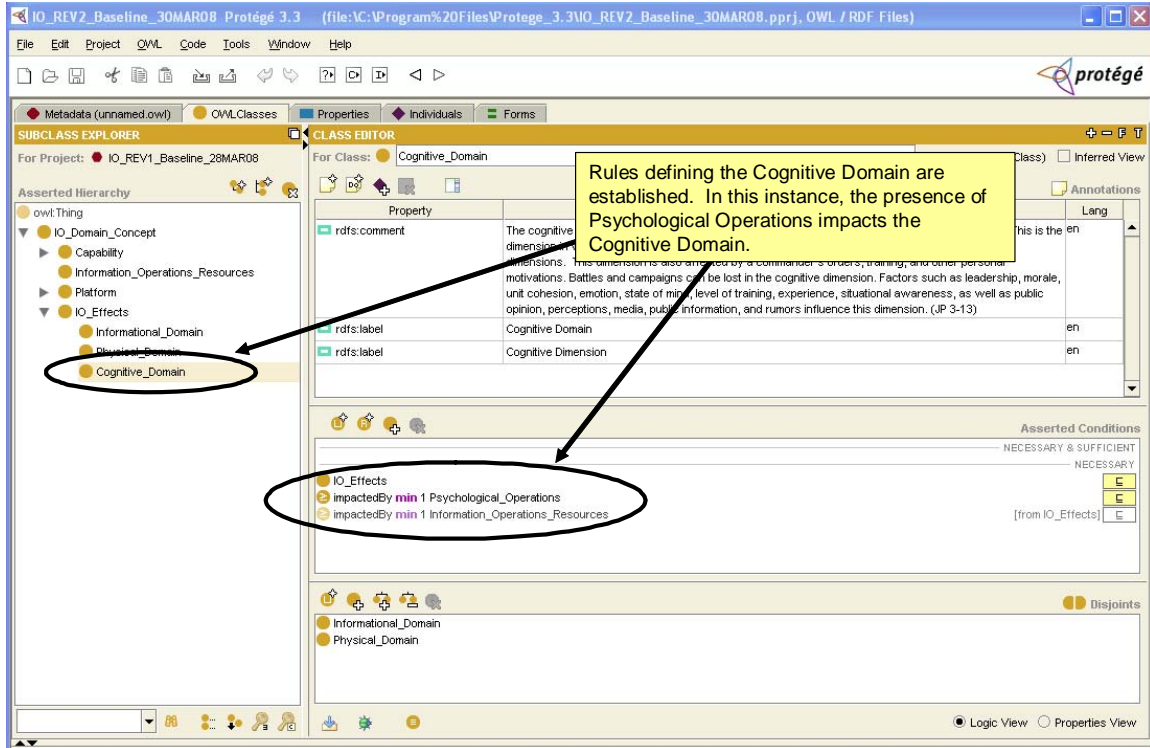
Figure 17.   Expansion of Rules to Encompass the Cognitive Domain.

D.   CONCEPT VALIDITY AND INTERNAL TESTING

In determining the Semantic Web potential of the ontology developed in the preceding chapter, there are two fundamental questions. The first is whether or not the logical assertions found in the ontology are accurate; the second is whether or not they are correct. The issue of accuracy is one of defining the domain as it really exists, whereas correctness is ensuring that the means to express the domain are not in error. Focusing for the moment on accuracy, this presents a bit of a dilemma. As there is more than one way of reasoning about a domain, there exists more than one way to accurately describe it.

Recognizing that accuracy is a critical underpinning to a valid ontology, the following are explanations for the rules that were used in this thesis.   While it is

understood that there are alternative ways of expressing the domain, the following represent an adaptive framework that are adequate to characterize much of the environment:

1) Information Operations Resources consist of a minimum of one capability and one platform. Further, an Information Operations Resource represents the union of these two entities. The utility of this is that the same USQ-113 jammer present on an EA-6B may also reside in a Light Armored Vehicle. This flexibility allows for a "mix-and-match" framework reflecting the manner in which many carry on components are employed.

2) All capabilities are associated with a minimum of one platform. A capability absent an associated delivery mechanism cannot be considered as an IO Resource. This rule ensures that capabilities are matched with a platform or platforms and is inherited throughout all Capability subclasses. A variation of this rule is apparent in both Leaflet Dissemination which is associated with Tactical PSYOP Battalions and the USQ-113(V)3 which is associated with the EA-6B. Note that these are not extended, but specifically applied to create definitive associations between designated capabilities and platforms.

3) All platforms are associated with a minimum of one capability. This is very much the mirror image of the preceding rule. This precludes the introduction of a given land, sea, air, or space platform without having an associated capability. The relationship between Leaflet Dissemination and Tactical PSYOP Battalions and the USQ-113(V)3 and EA-6B underscore this.

4) The final rule establishes that IO Effects are impacted by Information Operations Resources. The underlying rationale is that the application of some IO

asset would logically result in some effect in any one of the associated domains. Specifically, any combination of the Informational, Physical, or Cognitive domains.

These four rules serve as the firmament for the ontology to this degree of development. Moreover, no exceptions can readily be found. An EA-6B without associated capabilities does not present itself as an IO Resource. Leaflets are equally meaningless absent a means of delivery. This relationship holds true in all cases examined, and supports the first three rules. The final rule is intuitively obvious, as operations would not be undertaken without the intent to achieve some effect. Further, as the effects of IO are defined in three domains, these become the logical subclasses. The end result is that the expression of this domain is logically accurate.

The accuracy is predicated on the domain as structured, so it is reasonable to note that the domain could be expanded or reconsidered in such a way as to refute the validity of the rules as structured. By way of example, it would be equally acceptable to craft an ontology in which platform and capability were not disaggregated. Any reference to an EA-6B would assume the presence of a USQ-113. This would, of course, negate any value of the rule as established. However, as structured, the rules hold and, accepting their accuracy, the next question is one of correctness.

In this context, correctness is meant to refer to the degree to which the ontological and logical statements adhere to the rules of expression in the Ontological Web Language (OWL). One of the features available in the Protégé Ontological Web Language Editor is the ability to conduct ontology tests in order to identify any procedural faults in the associated code. If the test is run successfully, then the code can be accepted as being in the correct OWL format, meaning that it is suitable for use on the Semantic Web. The following figures illustrate the steps followed to conduct the ontology testing.

Step 1 – Establish Test Settings: prior to running the test, all Protégé ontology test settings were activated. Highlighted in Figure (18) are the specific OWL-DL tests conducted.
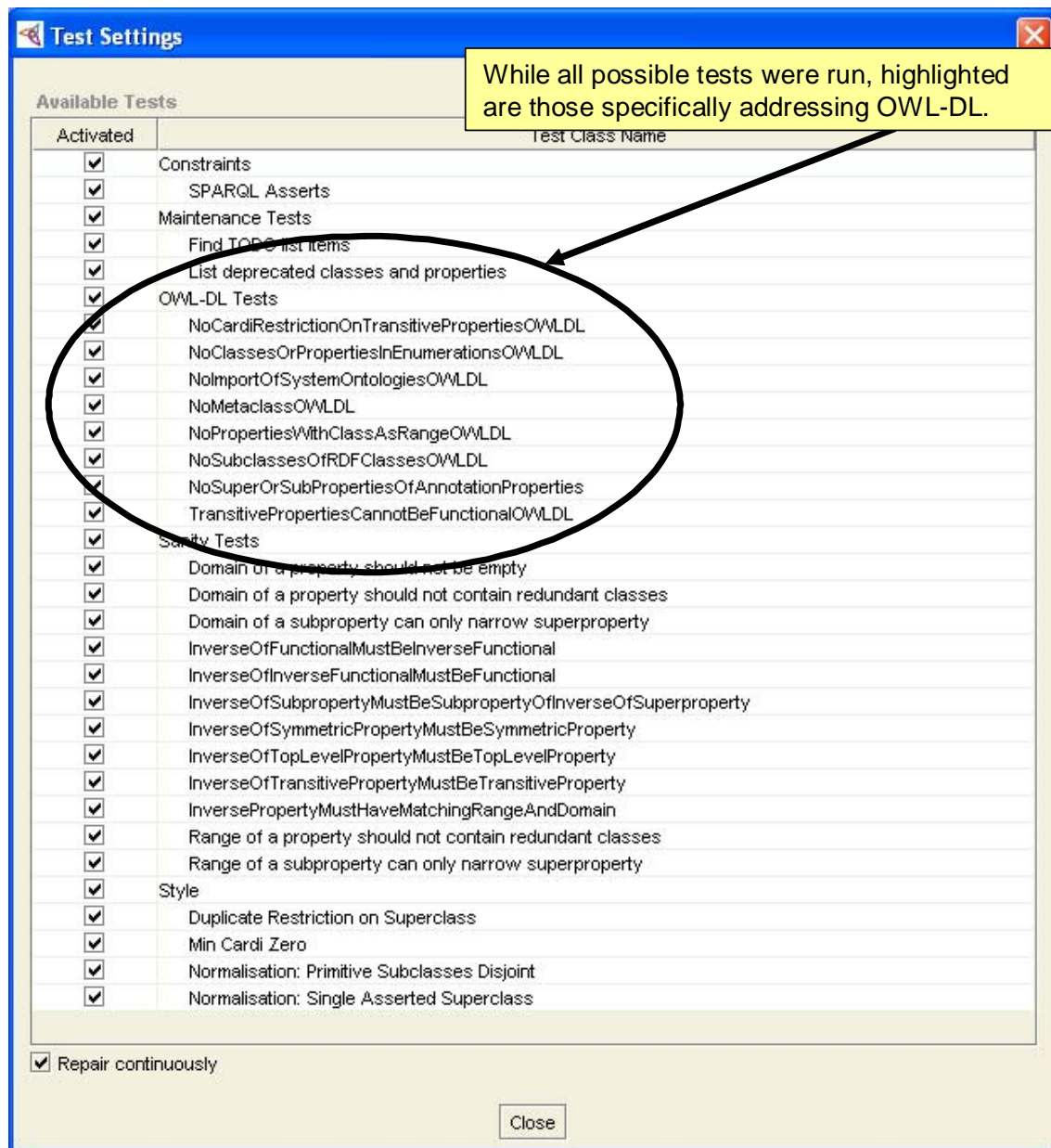

Figure 18.   Protégé Test Settings.

Step 2 – Execute the Test: having activated all test settings, the next step was to execute the test, as highlighted in Figure (19).
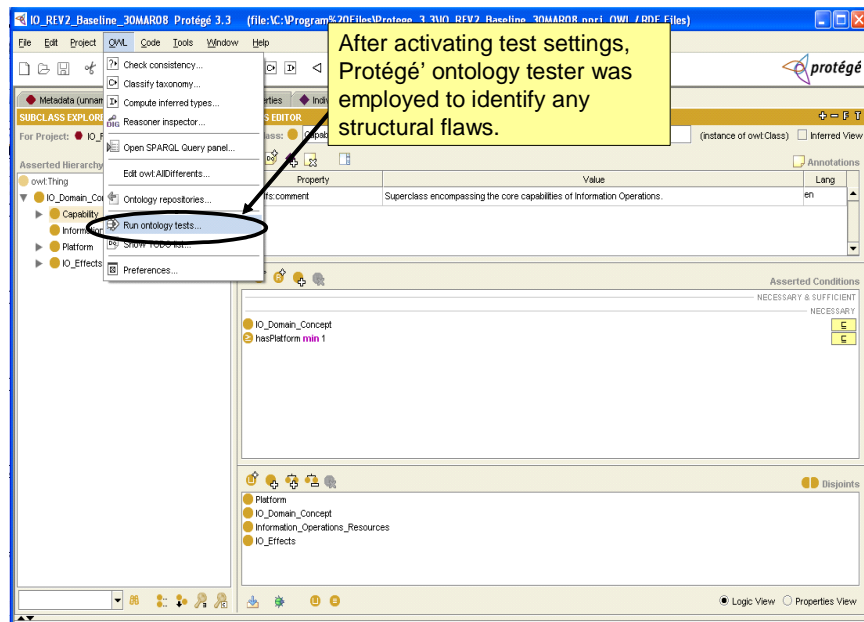

Figure 19.   Protégé Test Execution.

Step 3 – Interpret the Results: upon completion of the test, results were provided as depicted in Figure (20). As noted in the figure, there were no errors.
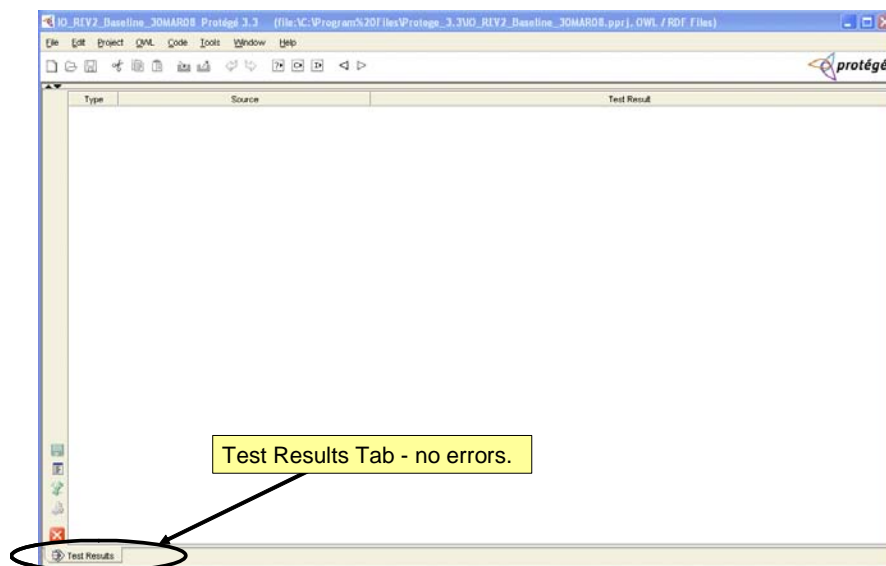

Figure 20.   Protégé Test Results.

E. TOWARDS THE SEMANTIC WEB

At the completion of the Protégé testing, the output was available in multiple formats. Appendices A and B contain the output in OWL and Java Schema. The following figures are captures of the output for use on the Semantic Web.
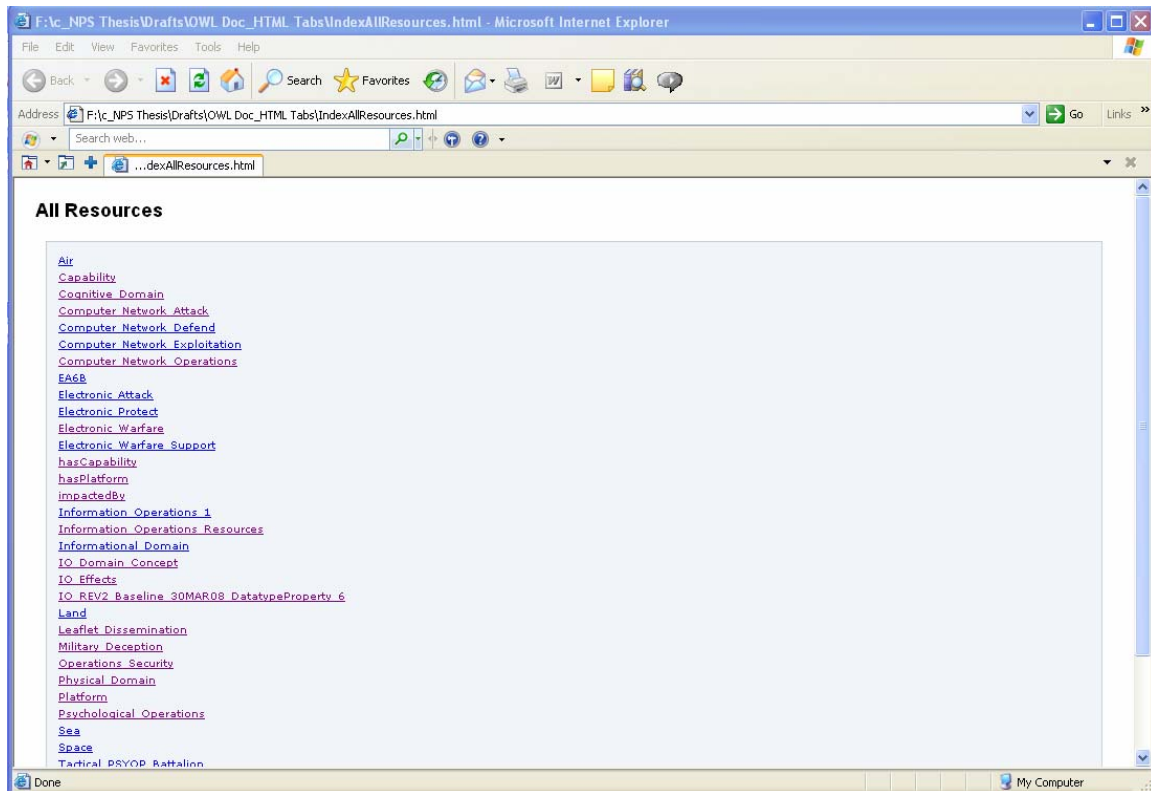

Figure 21.   Protégé Resource Tab.

Figure (21) contains all of the resources that are available within the IO Domain. Each of these is linked to other resources as established by the rules in the hierarchy. The following figures are returned when the Psychological Operations, Leaflet Dissemination, and Tactical PSYOP Battalion resources are selected sequentially.
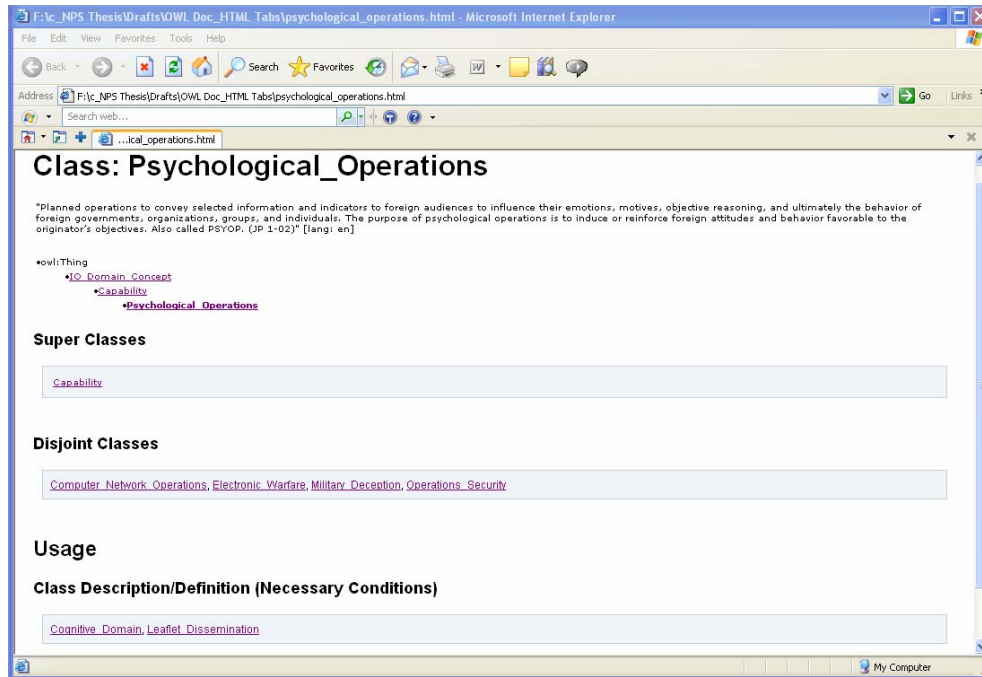
63

Figure 22.   Psychological Operations Class.
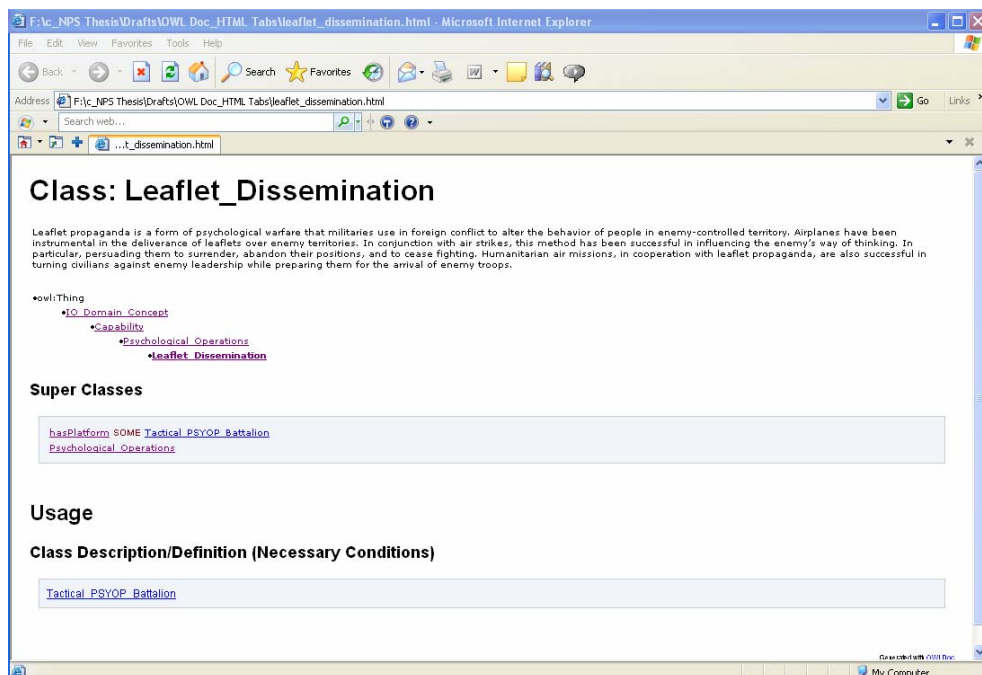

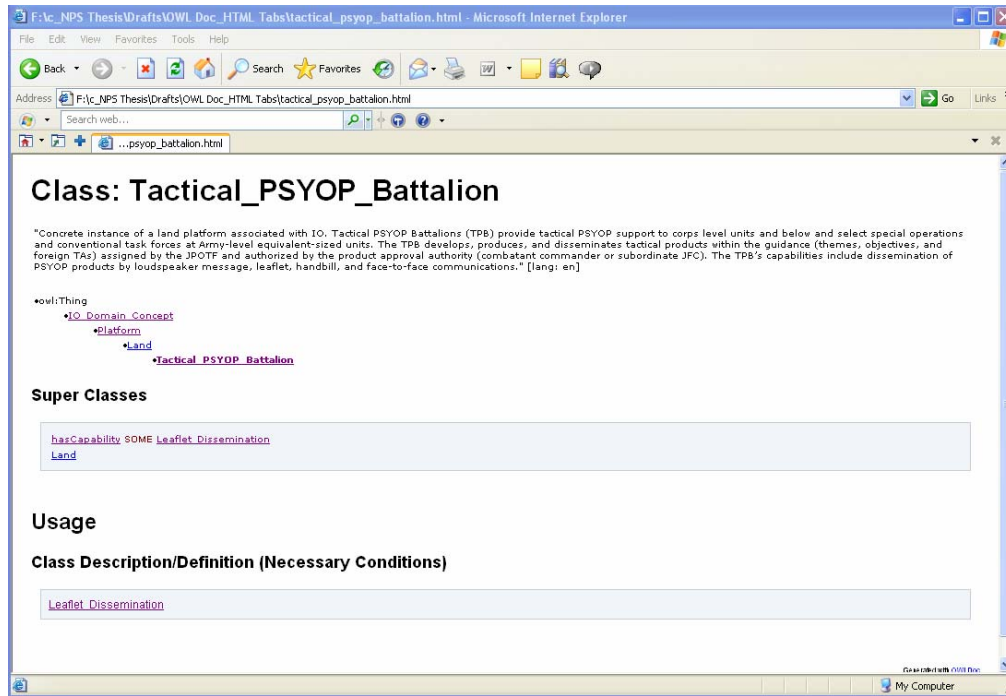Figure 23.   Leaflet Dissemination Class.

Figure 24.   Tactical PSYOP Battalion Class.

Similar pages were developed for each of the resources developed in the problem domain, with each reflecting the rules specific to the selected entity. The end result is that each of the classes and their associated relationships were sufficiently captured in OWL so as to be suitable for semantic publishing.

F.   ADDITIONAL METRICS AND VALIDATION

The testing conducted on the ontology has thus far emphasized the correctness of the code. While these tests are necessary, they are conducted within the development environment and results are provided on a pass or fail basis. Given the potential need for more quantitative metrics, the added benefits of exposure to alternative testing methods, and the ready availability of ontology testing tools, it is reasonable to employ a comprehensive battery of external testing applications to verify the outputs of the Protégé ontology editor. For the purposes of this thesis, the test battery includes Description Logic Expressivity, model metrics focused on classes and properties, and consistency checking of the ontology through external tools.

Description Logic Expressivity: Description Logics (DL) are used to represent the terminological knowledge of an application domain in a formal convention. Expressivity is captured through a translation into first-order predicate logic.[56] As this serves as a key element of ontology design, capturing the essence of the ontology in these terms offers a concise means of expressing the logic. The following figure, extracted from the Protégé metrics module, captures the DL Expressivity of the developed ontology:

The DL expressivity of this ontology is:

$$\mathcal{ALCQ}(D)$$

Symbol	Explanation
$\mathcal{AL}$	Allows concept intersection, full universal quantification, atomic negation and limited existential quantification (i.e. existential restrictions with fillers limited to owl:Thing)
$\mathcal{C}$	Complex concept negation (e.g. not(A or B)). Note that ALC allows disjunction and full existential quantification, which can be represented with conjuction and full negation, and universal quantification and full negation respectively.
$\mathcal{Q}$	Qualified number restrictions (qualified cardinality restrictions)
(D)	Datatypes

Figure 25.   DL Expressivity.

OWL Model Metrics: in addition to expressivity, there are other readily quantifiable attributes of an ontology. These are broadly expressed in terms of classes and properties, and facilitate a quick, top level comparison between two ontologies. This has utility in that it assists in assessing relative complexity and identifying common structural elements between ontologies. The following

---

[56] Liang Chang, Fen Lin, and Zhongzhi Shi. *A Dynamic Description Logic for Semantic Web Service. Semantics, Knowledge and Grid*, Third International Conference on Semantics, Knowledge, and Grid. 2007.

figure illustrates the specific metrics associated with the ontology developed in this thesis. These metrics were drawn from the Protégé metrics module.

Figure 26. Partial IO Ontology Metrics.

External Validation: thus far, all testing has been conducted through the Protégé application. In the interest of exposing the generated code to external scrutiny, there is some merit in employing multiple tools. To accomplish this, two additional tools were utilized. The first was the World Wide Web Consortium's

(W3C) RDF Validation Service[57], the second was the Project WonderWeb OWL Ontology Validator developed jointly by the University of Manchester, UK, Vrije Universiteit Amsterdam, Netherlands, and the University of Karlsruhe, Germany.[58] Collectively, these two tools plus the Protégé plug-ins offer a complementary means of verifying the consistency of the ontology.

W3C OWL Ontology Validator: The following three figures depict the process and results of the W3C validation. In Figure (27), the code is entered directly into the validator. Alternatively, this could be done by entering a URI for a specified document. The output options were set to graph only in order to provide a visual representation of the output. The results of the test, depicted in Figure (28) indicated that the ontology was consistent. The final figures are the graphed output of the validator service. Note that the scale of these graphs precludes framing them on a single page. Figure (29) provides an overview of the graph, while Figures (30) and (31) offer selected segments.

Figure 27.   W3C OWL Ontology Validator Code Entry.

---

[57] World Wide Web Consortium. "W3C Validation Service." <http://www.w3.org/RDF/Validator/> (accessed May 15, 2008).

[58] University of Manchester and University of Karlsruhe. "WonderWeb OWL Ontology Validator." <http://www.mygrid.org.uk/OWL/Validator>. (accessed May 15, 2008).
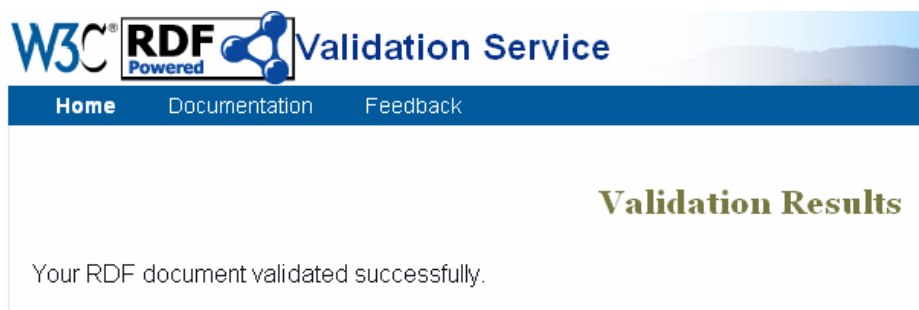
Figure 28.   W3C OWL Ontology Validator Results.
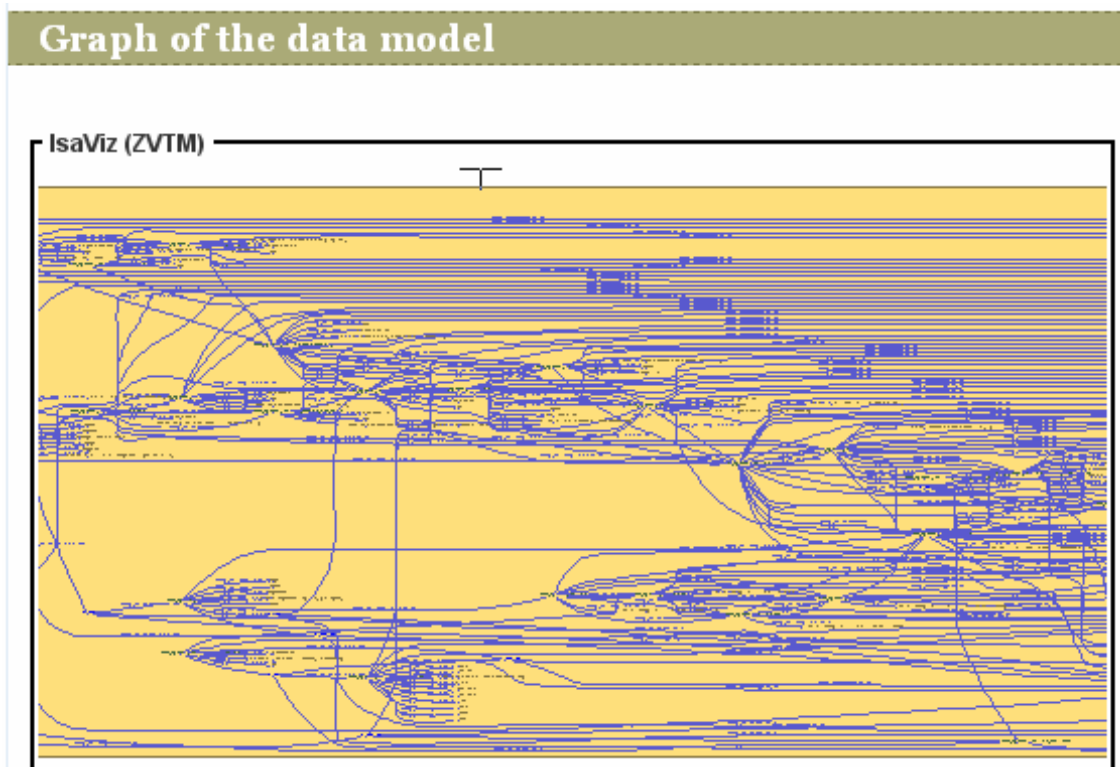
Figure 29.   W3C OWL Ontology Validator Overview Graph.
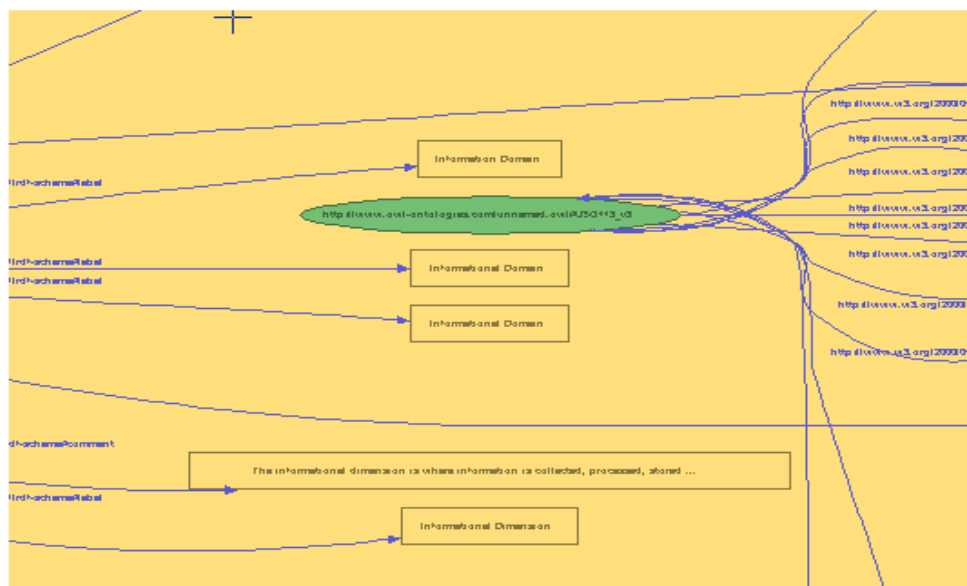
Figure 30.   W3C OWL Ontology Validator Overview Graph Excerpt 1.
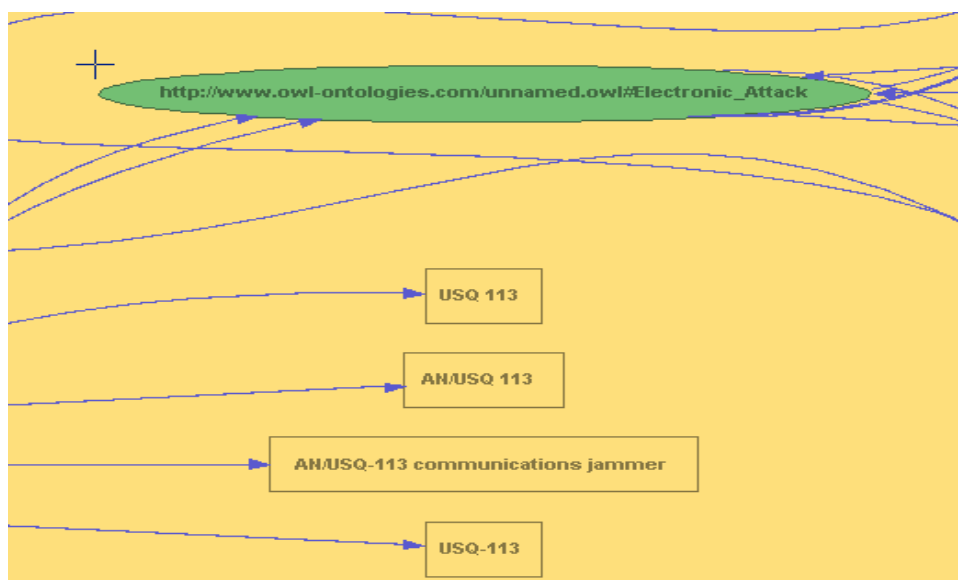
Figure 31.   W3C OWL Ontology Validator Overview Graph Excerpt 2.

Wonder Web OWL Ontology Validator: this tool provides a service similar to that provided by W3C with two exceptions. The first is that it characterizes the type of code entered as a specific OWL variant and the second is that it presents amplifying data in terms of specific constructs used and converts the OWL to an abstract syntax form. The following figures illustrate the data entry, OWL species characterization, the constructs used, and abstract syntax.

Figure 32.   WonderWeb OWL Ontology Validator Data Entry.

Figure 33.   OWL Species Validation Report.

Figure 34.   Constructs Used in the Ontology.

Figure 35.   Extract From the Abstract Syntax Form.

As often stated, you can only control what you can measure, and ontologies are no exception to this rule. Accurate metrics allow for both the assessment of an ontology and provide the capacity to track their evolution. One of the recurring challenges on this front is that many of the tools for evaluating ontologies do not fully consider the semantics of

the ontology language into account.[59] While the small battery of tests conducted in this chapter is far less than what may be required for a formal test plan, they have illustrated several key concepts for ontology testing. These concepts include consistency checking, classifying the OWL species, identifying key constructs, developing taxonomies of classes and properties, logical expression, and visual graphing of the ontology. While certainly not exhaustive, these elements provide a strong basis for evaluating ontologies.

G.   VISUALIZATION AND DOCUMENTATION

While the preceding sections have identified a developmental framework, they have not addressed the range of visualization and process documentation tools available to the developer. While in practice these activities would be ongoing throughout the development cycle. The discussion was placed later in the chapter specifically to treat them separately, and is not intended to connote that they are in any way less important. In order to illustrate the range of visualization options, this section will apply several views available through Protégé plug-ins. Process documentation will be based on extracting the code from Protégé as an .XMI file, which can be uploaded into a separate application called Poseidon, a popular Unified Modeling Language (UML) editor. Poseidon is able to upload the .XMI file provide an automated means of translating the ontology developed in OWL to be expressed in UML. While this is not a fully automated process, it significantly reduces the level of effort associated with documentation.

> **Visualization**: The following figures were developed using various views available in the Protégé tool, and can be used to support the requirements of various participants in the development process. Note also that many of these tools also have the capability to be manipulated by the user, allowing for direct interaction and manipulation of the ontology.

---

[59] V. Cross and A. Pal. Metrics for Ontologies. Fuzzy Information Processing Society, 2005. NAFIPS 2005. Annual Meeting of the North American Fuzzy Information Processing Society. 2005.
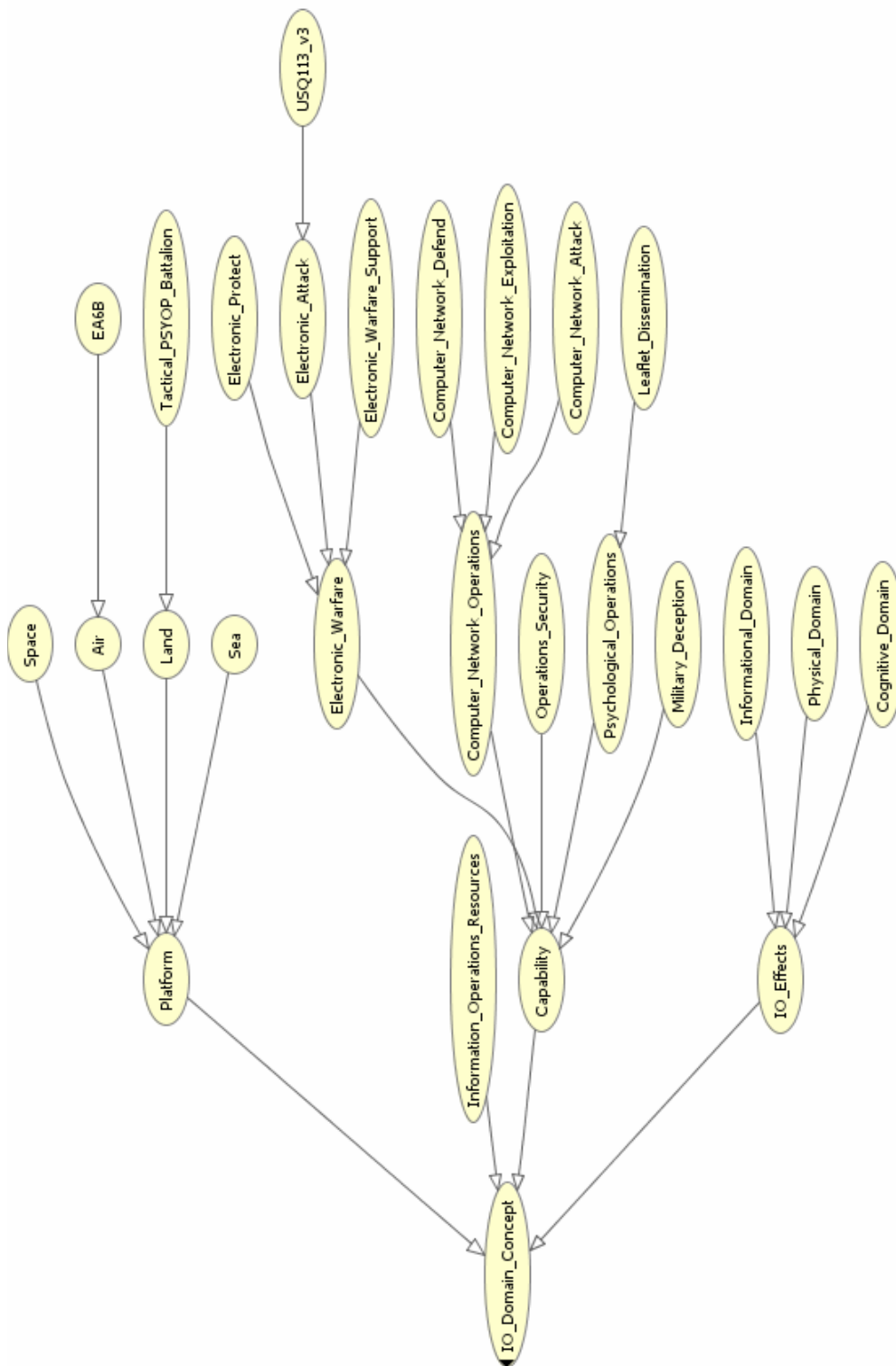
Figure 36.   Protégé OWLViz Hierarchical Diagram.
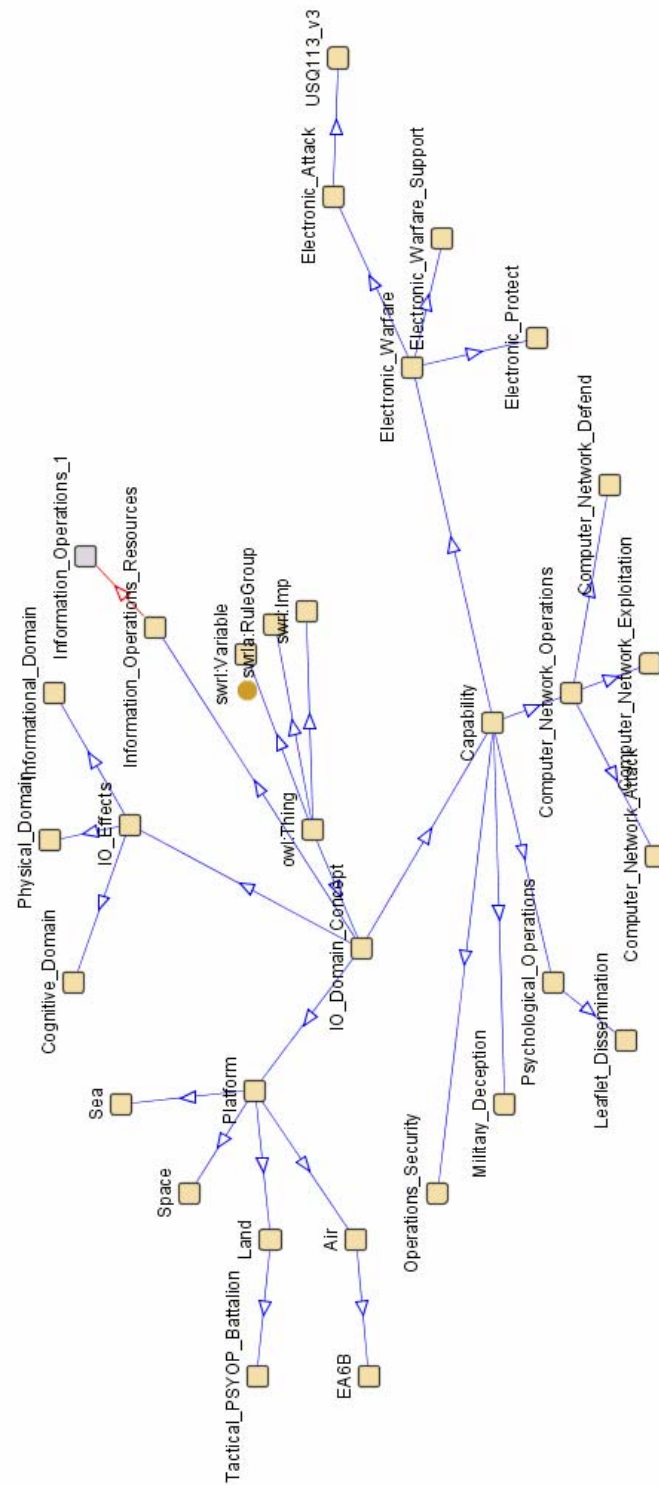
Figure 37.   Protégé Jambalaya Radial Layout.
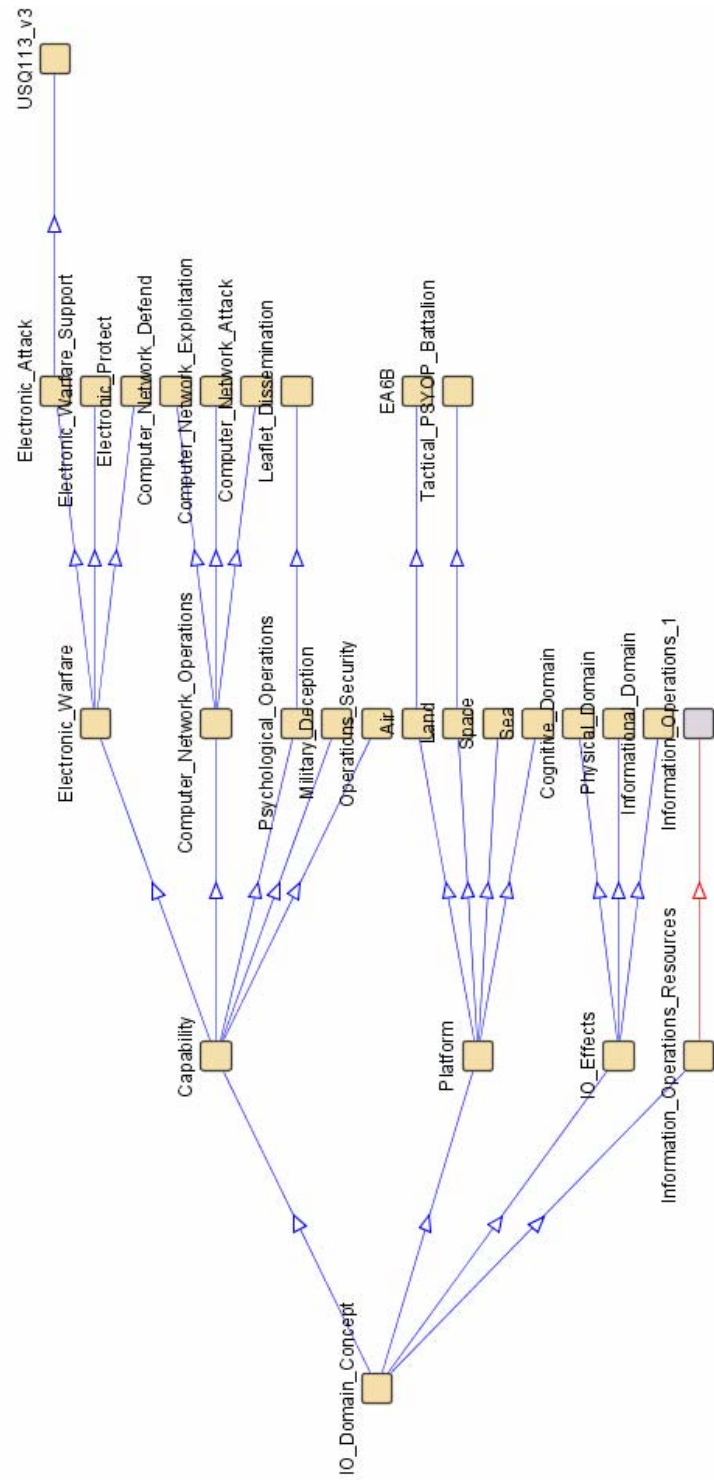
Figure 38.   Protégé Jambalaya Horizontal Tree Layout.
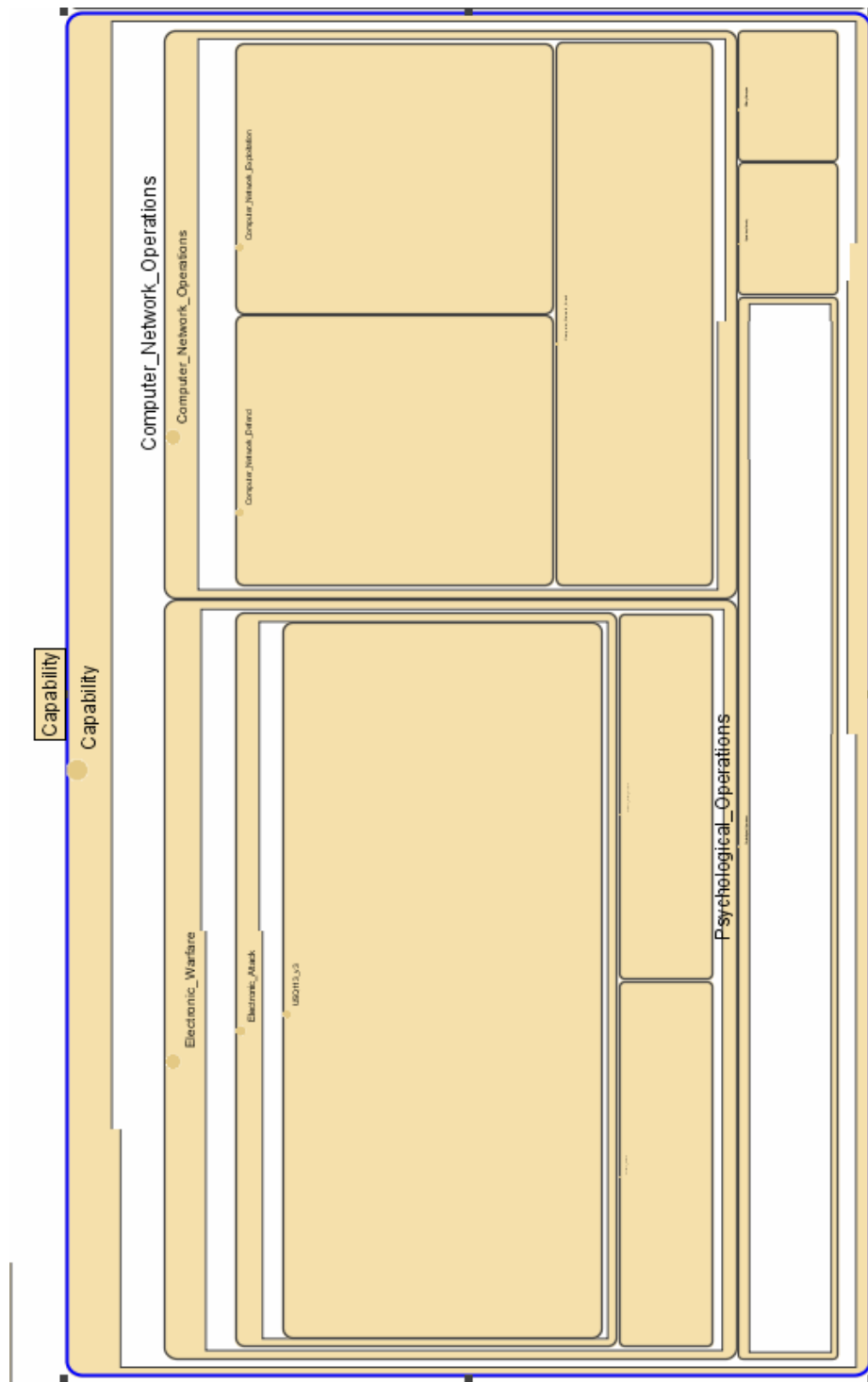
Figure 39.   Protégé Jambalaya Nested Tree Map (Partial).
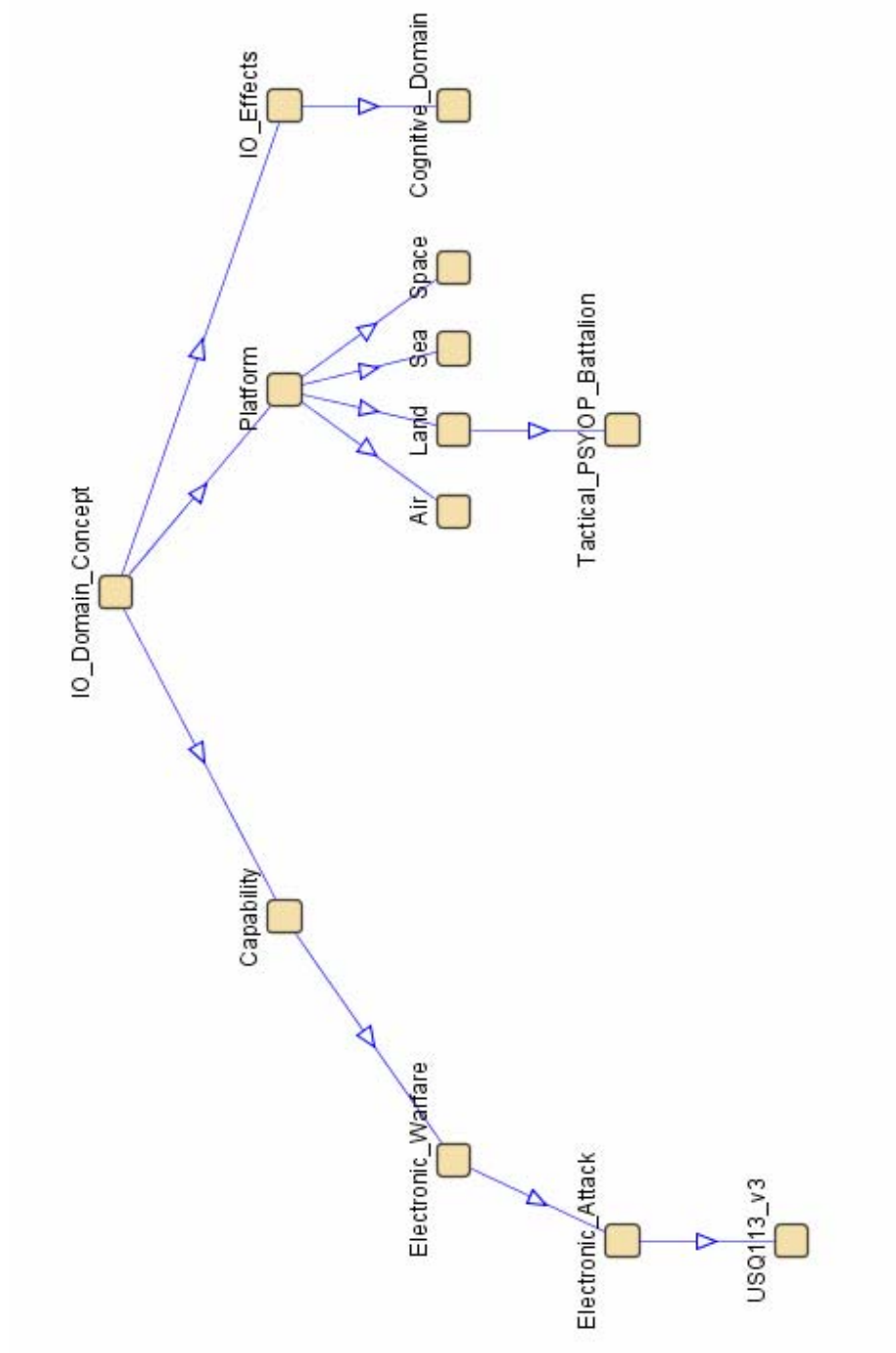
Figure 40.   Protégé Jambalaya Hierarchy Tree (Partial).
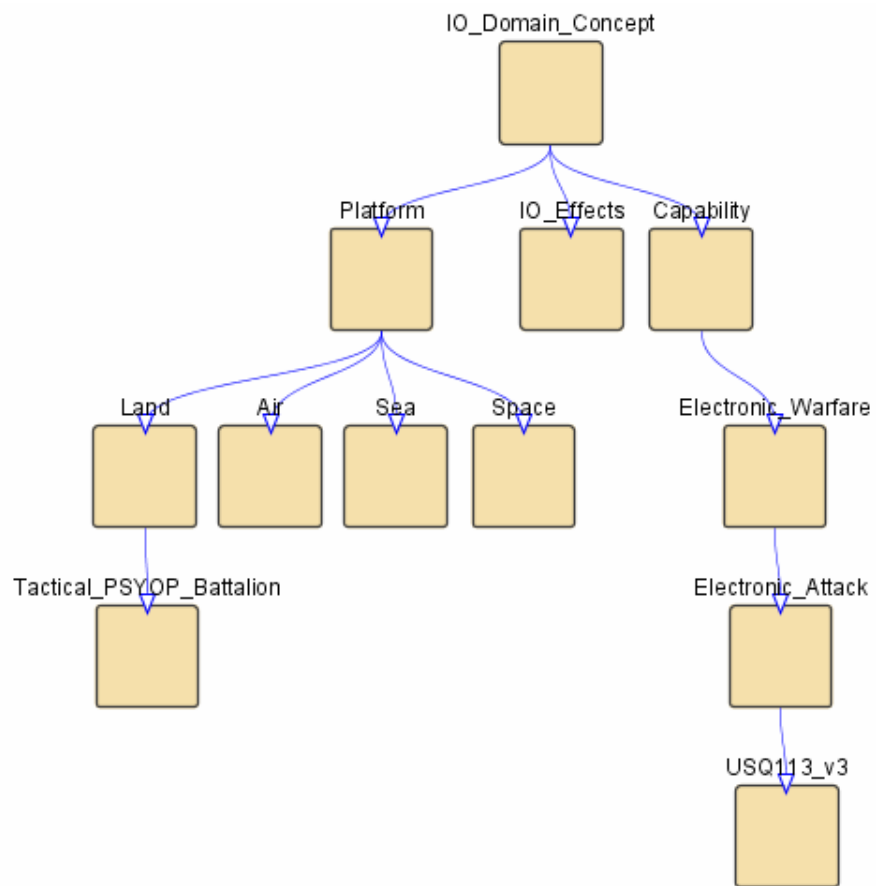
Figure 41.   Protégé Jambalaya Sugiyama Layout (Partial).
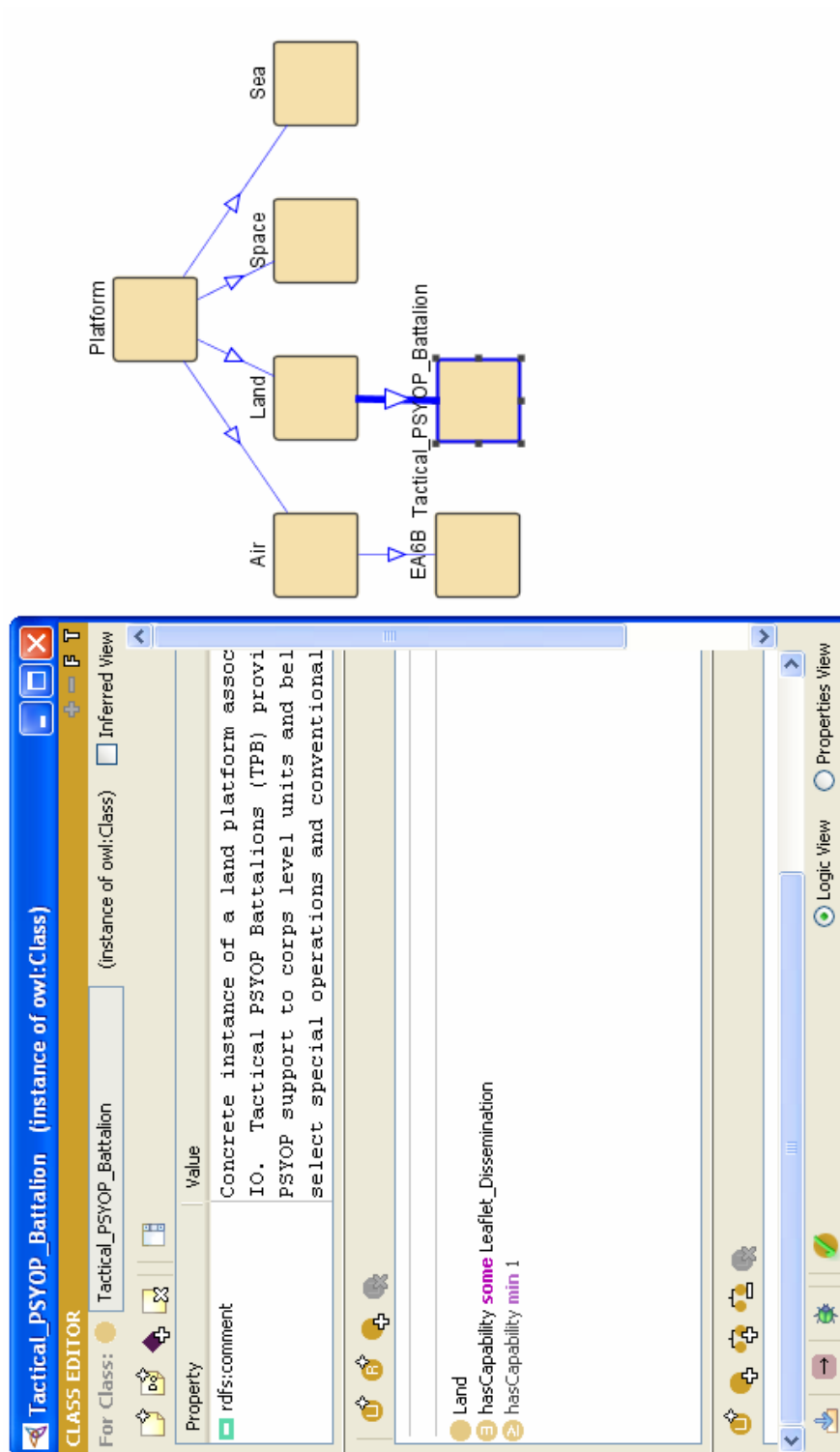
Figure 42.   Protégé Jambalaya Expanded View.
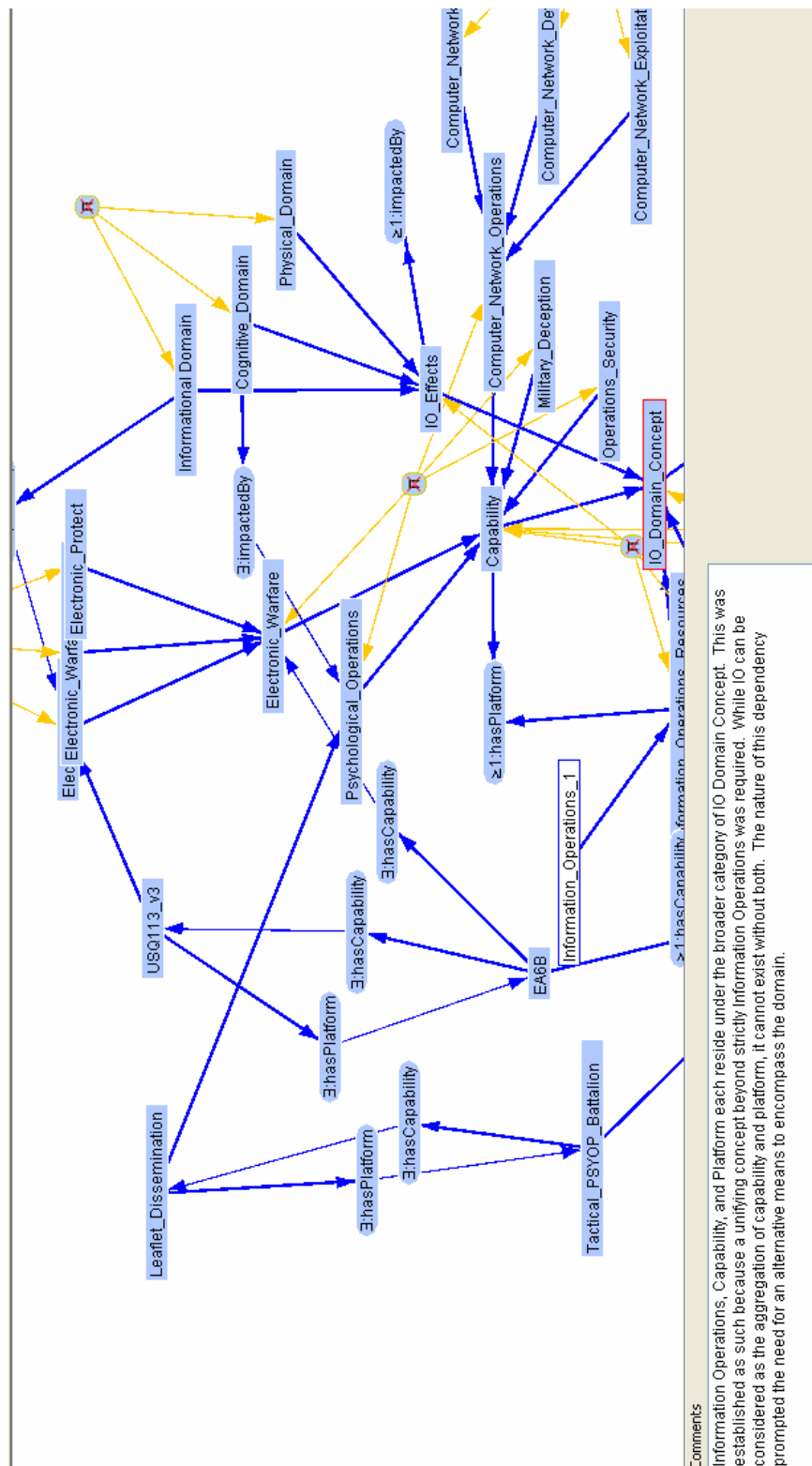
Figure 43.   Protégé GrOWLView.

Documentation: The visualization tools are of significant utility in both development and documentation. In and of themselves, however, they do not constitute a truly standardized means of documentation. To facilitate both the ease and standardization of documentation, both the Protégé and Poseidon tools were used. The former served as the ontology editor and the latter provided a means to develop UML diagrams. By using Protégé's conversion features, the OWL file could be exported as an .XMI file which could be used by Poseidon. The following set of figures illustrates the means by which this can be achieved.
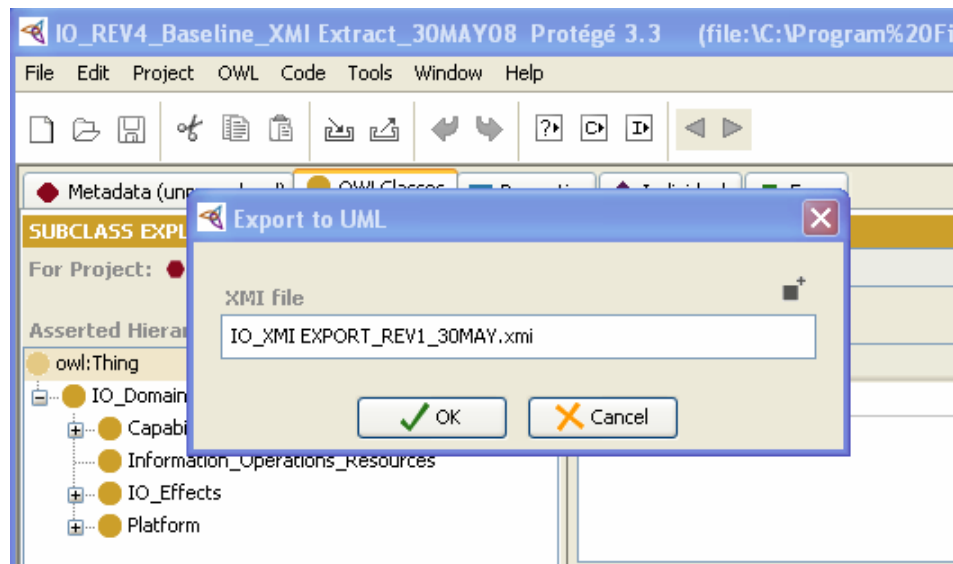
Figure 44.   Conversion to .XMI Format in Protégé.
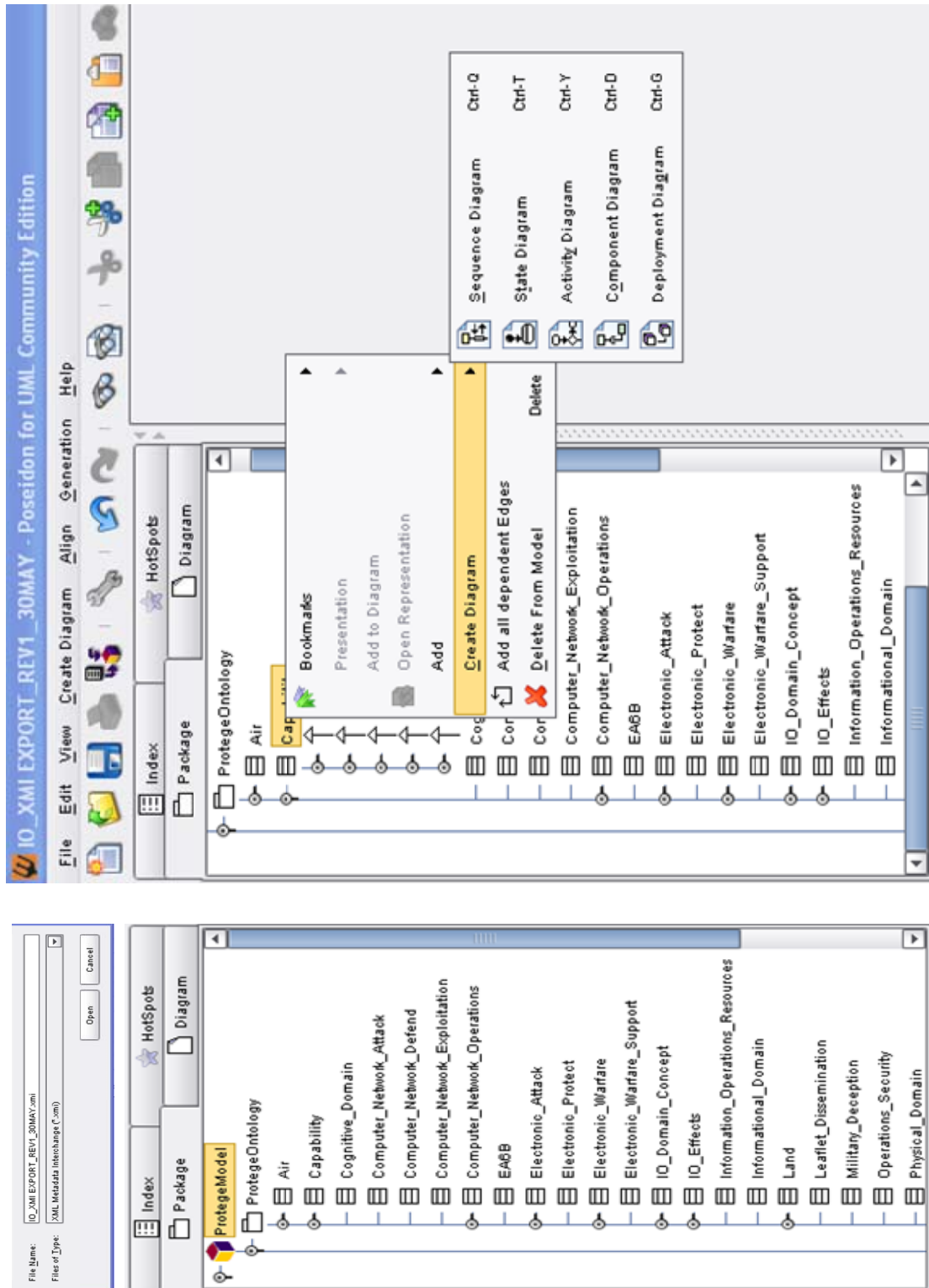
Figure 45.   Import XMI File Into Poseidon and Create Diagrams.
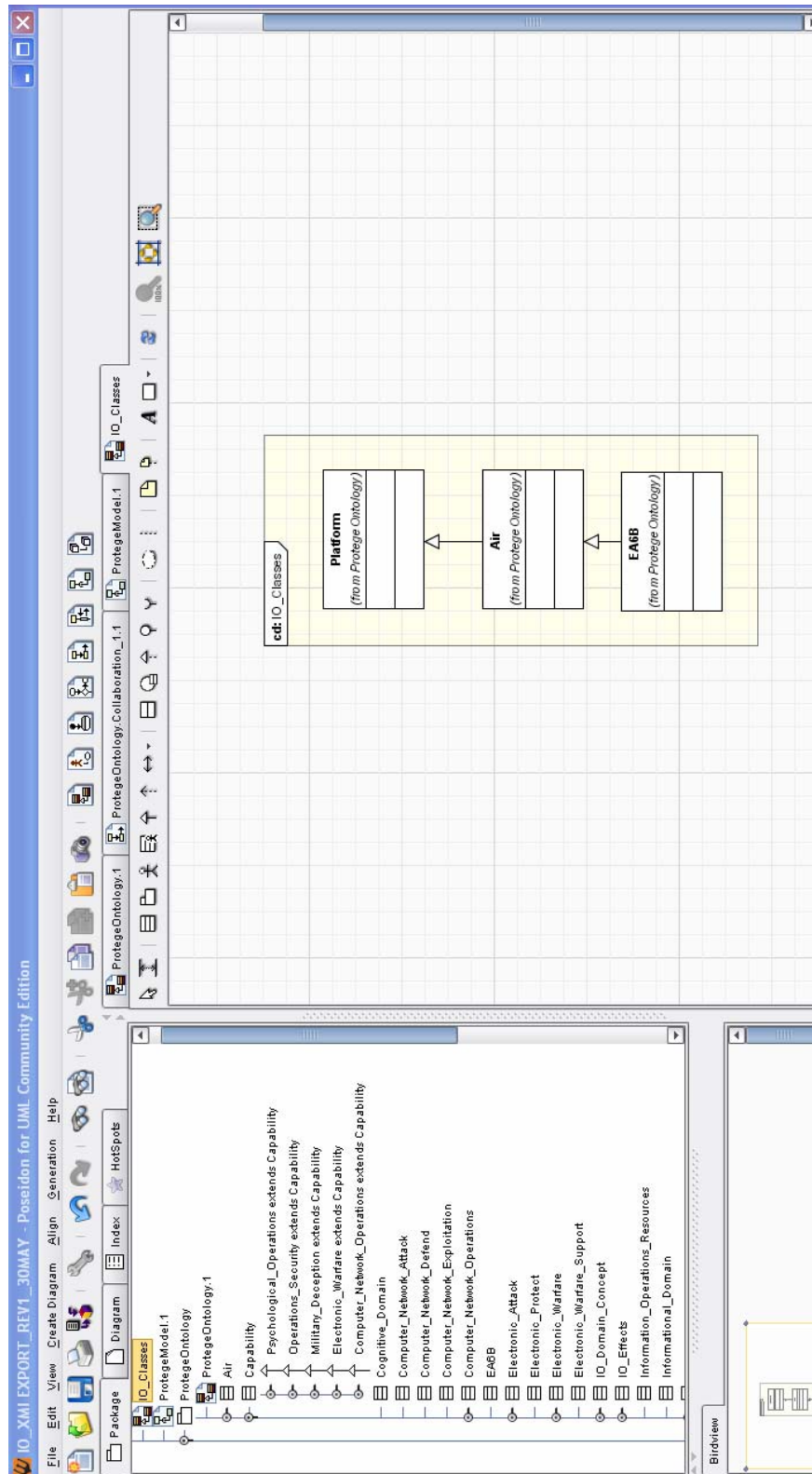
Figure 46.   Create Class Diagrams.

84
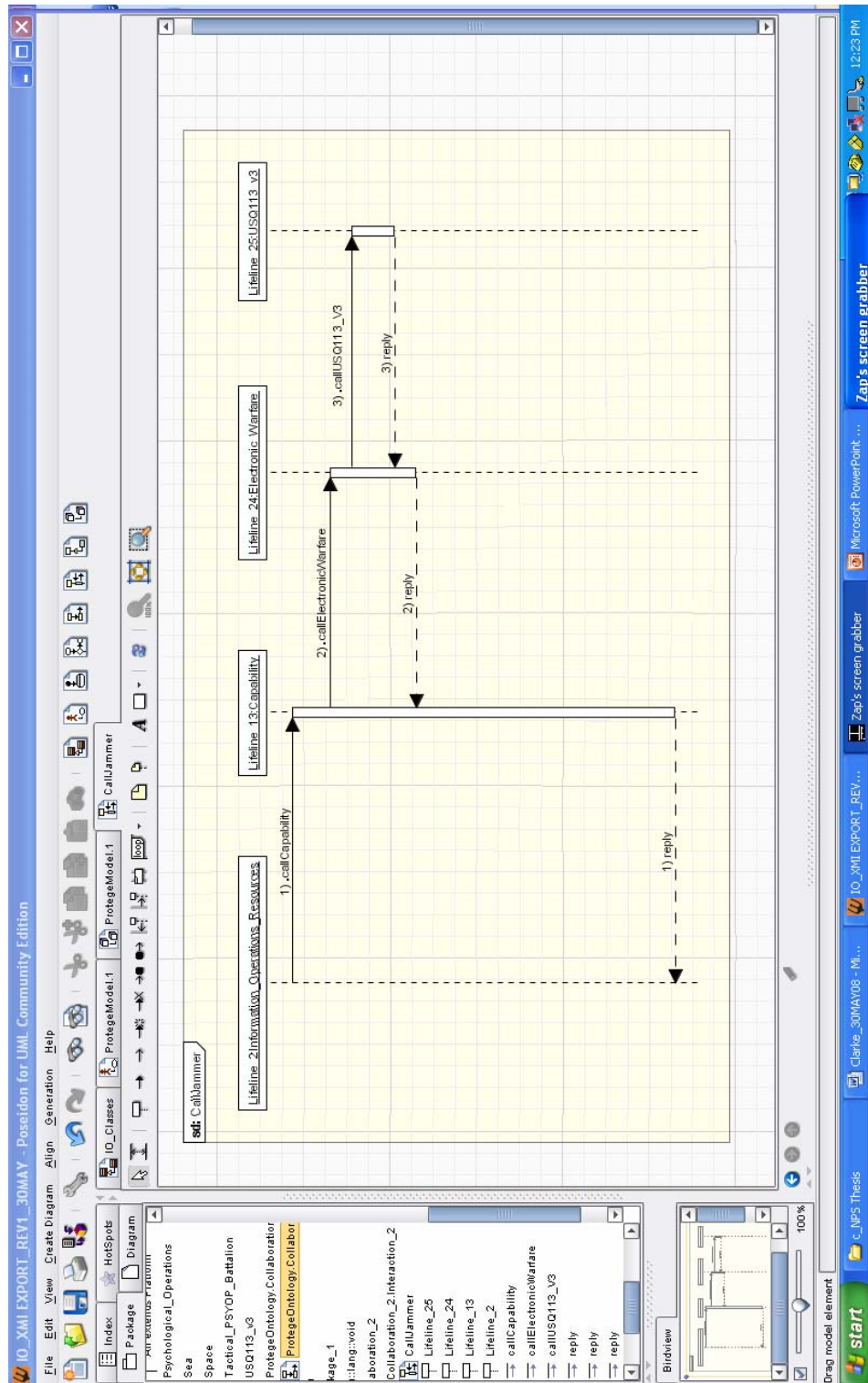
Figure 47.   Create Sequence Diagrams.
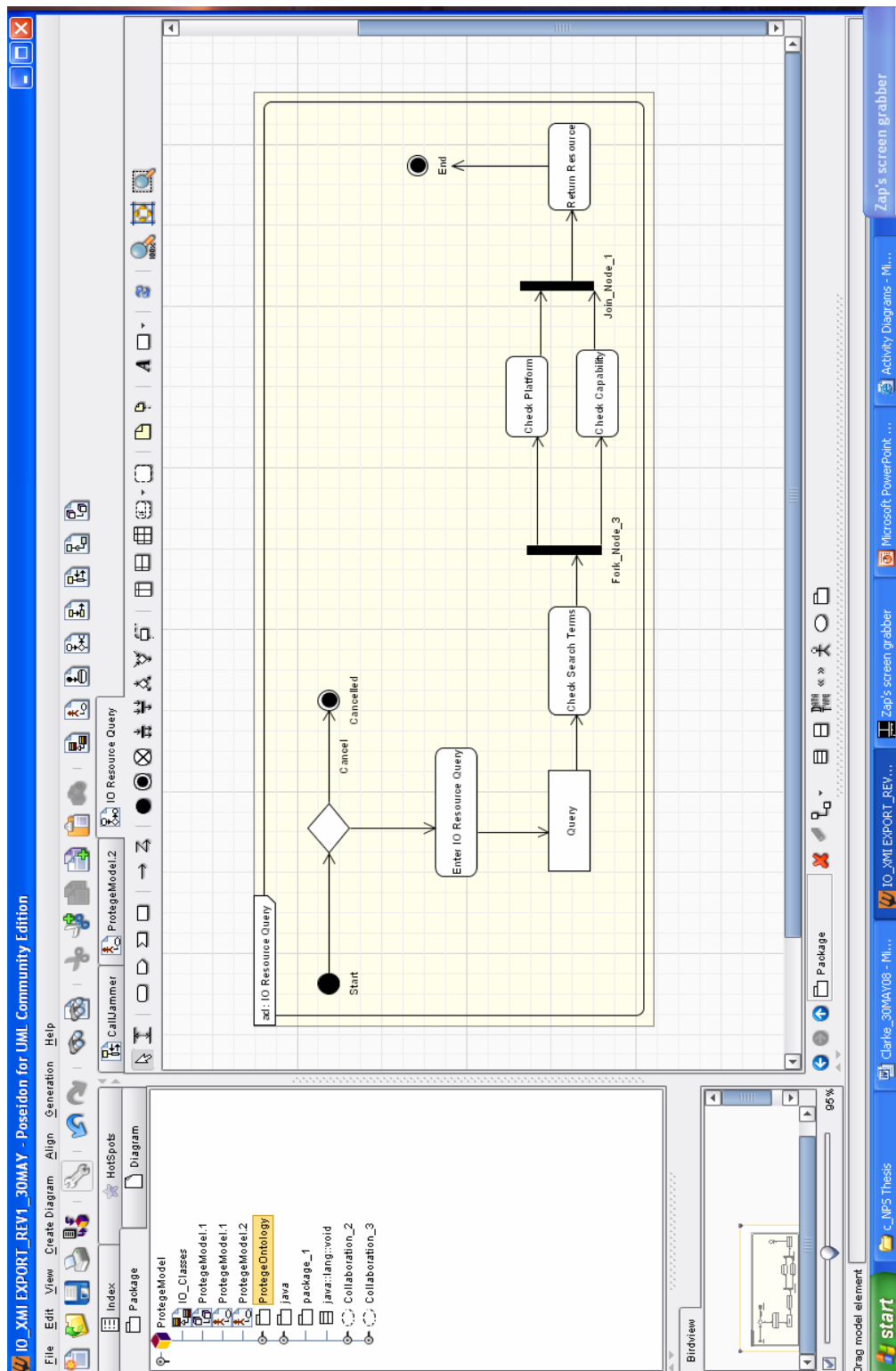
Figure 48.   Create Activity Diagrams.

The discipline of engineering entails measurement and documentation. Regarding the latter, the Unified Modeling Language has become a key tool for expressing software concepts in a widely accepted form. Given the capacity for an ontology editor, in this case Protégé, to be able to directly export domain concepts to a UML editor reduces the level of effort associated with documentation. This allows for multiple views to be readily developed and facilitates a broader sharing of ideas and scrutiny. The methods described in this section are one way to increase the ease and fidelity of program documentation.

H. CONCLUSIONS

Ontologies are effectively a reasoning framework within which domain knowledge can be considered. However, there is no singular way in which a given domain must be considered. As a result, ontologies representing the same domain may vary significantly. This should not imply, however, that all ontologies are equivalent in terms of utility. To craft an adaptive ontology, the reasoning framework must be anchored in a set of abstractions that can consistently be used to represent the problem domain.

In the context of the framework developed in this chapter, the overarching IO Domain Concept is characterized by resources and effects. The concept of IO Resources is an aggregation of platforms and capabilities, allowing for a broad range of interaction between multiple types of assets. Effects are characterized by their impact in one of three domains, Informational, Physical, and Logical. These effects are achieved by applying an IO resource. So, although a minimal amount of concepts have been introduced and only a few rules applied, it begins to become apparent that the larger Information Operations domain can be generally characterized within the bounds of the ontology. To increase the fidelity and accuracy of the model, it becomes a matter of introducing new rules and expanding the available classes. Even with the limitations of this framework, this is still an adequate point of departure for evaluating its suitability for use on the Semantic Web.

The test results confirm the structural correctness of the OWL output associated with the developed ontology, thus illustrating its suitability for use on the Semantic Web.

However, a caveat needs to be applied. Although the logical foundations are accurate and the associated code is technically correct, in its current iteration the ontology is of limited utility. While the classes and rules developed this far are sufficient as a starting point for characterizing the IO domain, it does not contain enough fidelity for practical use, and nor was this the intent of the thesis. What has been illustrated is a means by which the IO problem domain can be developed within an ontological structure suitable for use on the Semantic Web.

VI. CAPTURING THE PROCESS

The Semantic Web will bring structure to the meaningful content of Web pages, creating an environment where software agents roaming from page to page can readily carry out sophisticated tasks for users.

T. Berners-Lee, J. Hendler, and O. Lassila
The Semantic Web

A. DEFINING THE METHODOLOGY

In the preceding chapters, several steps were taken that led to the creation of a partial ontology of the Information Operations problem domain. By re-examining these steps, a more explicit methodology can be constructed that lends itself to greater repeatability. The following constitute the steps taken in the construction of this ontology:

1) Comprehensive Domain Analysis: Prior to developing any problem domain into an ontology, it needs to be considered broadly. As the ontology is ultimately intended to bride the gap between man and machine, it is essential that the concepts developed by humans are understood by the ontology developer. Absent this, the risk is one of a technically correct but conceptually inaccurate output. For this thesis, domain analysis consisted primarily of a review of relevant IO and ontology development literature. The study of the former provided a means to better understand the problem domain, while the latter allowed for the identification of relevant tools and best practices.

2) Establish Doctrinal Links: The challenge of a broad study of the domain is one of scope. The more material that is reviewed, the more links and interactions become unearthed. While this expansion represents an increase in scale and is in many cases necessary, if embraced too soon the scope of the initiative will quickly become unwieldy. In this instance, the means of managing scope was to

ground the ontology in the current IO doctrine. The joint publications surrounding this discipline constitute the settled knowledge in the problem domain and are what IO practitioners refer to gain knowledge. Given this, it is practical to use doctrine as a means to ground the initiative. Note that this does not negate the need for a more expansive domain analysis, as the concepts presented in other documents allow for a broader contextual understanding which is of significant assistance in characterizing the domain.

3) Identify the Highest Level of Class Aggregation: The concepts presented in doctrine are intended for human consumption. In some instances, this may be suitable for use in framing the ontology, but in other cases it may not. By identifying the threads of commonality that link seemingly disparate concepts, a more concrete means of expression becomes available. In this instance, "platform" became the aggregation of air, land, sea, and space. "Capability" became the aggregation of how a given IO asset contributes to operations. With as few as two elements of aggregation, it is possible to basically characterize all IO resources in explicit terms.

4) Characterize Relationships between Classes: Once the levels of aggregation are established, it becomes necessary to establish how the respective classes interact with each other. This is a fairly extensive process as the possible relationships can be quite large, but generally finite. To elaborate on this, while software can create any type of reality, and ontology is a model of the real world. Relative to this thesis, we know that a Tactical PSYOP Battalion is not a capability resident on an EA6B. This allows for descriptive rules to be developed to characterize relationships, which will later translate into the ontology.

5) Enter Domain Concepts into an Ontology Editor: In this case, the development of the ontology served the larger purpose of modeling elements of the IO domain with sufficient fidelity so as to be suitable for use on the Semantic

Web. To achieve this, the ontology needs to be expressed in a manner more understandable by machines. The mechanism for achieving this is through the use of an ontology editor. In this case, the Protégé tool was used as it was easily accessible, had a relatively wide body of users and established support, and numerous plug-ins had been developed to expand its functionality. Further, it allowed for the conversion of file types into a variety of formats which supports further manipulation. Once the concepts are captured in the ontology editor, conditions are then set for assessment.

6) Testing the Ontology: The degree of testing required is in part dependent on the nature and use of the ontology. It suffices to say, however, that for an ontology to be suitable for use on the Semantic Web, some level of testing must occur. Testing for the proper characterization of the problem domain is an activity best served by exposure to domain experts beginning with domain analysis and continuing throughout development. This is a manual means by which humans verify the correctness of the information that will be captured in the ontology.

Testing for the technical correctness of the ontology and any generated code becomes a more automated process and will vary relative to the tools available. At a minimum, the ontology should be checked for logical consistency through the use of any number of widely available tools. While testing needs may vary, it may also be beneficial to capture Description Logic Expressivity, metrics on ontology classes and properties, and specific performance characteristics relative to search accuracy.

7) Visualization and Documentation: Positioning these two practices at the end of the sequence is not meant to imply that they are of lesser importance. The activities should continue throughout the development cycle in a manner prescribed by local practices. Note also that visualization and documentation tend to complement each other in that a great deal of contemporary documentation

employs visual tools. Visualization tools provide a means to express a domain in a readily understandable format. Further, the depth and breadth of many visualization tools facilitate multiple views relative to the needs of a given user.

In terms of documentation, this can be done in a variety of ways, but UML seems to offer significant advantages. In addition to its largely visual nature, it is widely accepted and is supported by a variety of tools. The methods employed in this thesis allowed for the export of the ontology directly into a UML editor, facilitating a degree of semi-automated artifact development.

B. CONCLUSIONS

Process engenders stability. While the steps described in this chapter are far from prescriptive, they do offer a broad framework for ontology development and are illustrated by the actions taken and described in the preceding chapters. There is, of course, more than one way to accomplish any task, but taken collectively the methodology outlined in this chapter is a reasonable point of departure for ontological development, particularly in the IO problem domain.

VII. CONCLUSIONS

The enemy must not know where I intend to give battle. For if he does not know where I intend to give battle he must prepare in a great many places. And when he prepares in a great many places, those I have to fight in any one place will be few.

Sun Tzu
The Art of War

A. BROADER IMPACTS

The primary purpose of this thesis has been to illustrate how Information Operations capabilities may be represented in a software ontology and identify a process through which an IO ontology may be adapted for use on the Semantic Web. While this has been achieved, the associated utility of this approach remains to be seen. The immediate benefit can be found in expressing concepts in such a way that they can be understood by machines, but the larger question of its practical application remains unanswered.

The answer to this can be found in the innate capabilities of computers, specifically their relative speed. If the concepts of the IO domain can be accurately expressed in a machine understandable format, the machine can consider what combination of resources are best suited to achieve the desired effect in a fraction of the time required by humans. Thus, the overarching advantages of this approach are found in the combined speed and accuracy computing power can bring to bear. The combined advantages of speed and accuracy translate into swifter and more precise application of resources coupled with more predictable effects.

Given the benefits that an ontological approach may offer, the intuitive question is how to realize it. While the model presented in this thesis has illustrated one approach, to implement this on a larger scale would require a much wider range of systemic changes. To achieve this reality, a combined approach encompassing the manner in which doctrine is developed, ontologies are constructed, and rules are defined would need to be employed. The following sections will address specific conclusions that have been reached regarding each of these factors.

B. DOCTRINAL IMPACTS

In the context of this thesis, ontologies are a means of abstractly representing the IO problem domain. In this regard, an ontology is not dissimilar from written language, which is an abstraction in its own right. Regarding the latter, the Department of Defense employs an extensive apparatus and lengthy processes to develop doctrine that is intended to be understood by humans, not machines. In this regard, the system is quite effective. Doctrinal publications have provided the basis for much of the IO domain knowledge in this thesis. Collectively, they offer a strong means of characterizing a discipline for humans, not machines.

A significant change that is required is found in the scope of doctrinal development. In addition to defining doctrine in written terms, an accompanying set of logical rules that define doctrinal concepts in the context of the warfighting functions it serves should be developed in parallel. This approach would mend the seam that is often resident in translating domain information to software applications after the fact. As domain knowledge is captured in doctrinal publications, an accompanying set of publications should be provided to define the terms and concepts in a manner that can be understood by machines.

This doctrinal companion document would take terms and concepts and assign semi-formal rules that place them in the context of the relationships it maintains with other entities. By having rules and context associated with terms at the outset, conditions are better set to accurately develop, update, and refine ontologies to ensure a faithful representation of reality in a format that can be understood by machines. If this is established as a condition of doctrinal development, domain knowledge can be captured as it is developed.

C. ONTOLOGIES

The preceding section addresses a general methodology and an ideal point in time at which domain knowledge may be represented in a machine understandable format. If accomplished, this provides a machine understandable lexicon from which ontologies can be developed. Given that these machine understandable terms form a type of reusable

component, the next challenge is to place these components in some type of meaningful framework. This framework is the ontology, and the manner in which it is structured partially defines its utility.

As noted in previous chapters, problem domains can be expressed in multiple ways, meaning that significantly different ontologies can be used to express the same domain. Given that there are several approaches to develop the ontology, ontological development becomes a practice that benefits more from best practices rather than a strict set of guidelines. While this is far from prescriptive, the following are some conclusions reached in developing this thesis:

1) The ontology should be able to be easily changed. Domain knowledge is dynamic. New terms and concepts are constantly developed, and with each change relationships between entities are altered. To preserve the utility of an ontology, it needs to be flexible enough to adapt to change.

2) Adaptability in ontologies is well served by defining a level of abstraction that is broad enough to encompass meaningful concepts but narrow enough to convey immediate context. By defining ontologies in this manner, "concrete" rules can be established to govern higher levels of abstraction. Subclasses can be governed by these rules and extended as required to accommodate specific relationships between entities.

3) Variations on relationships preclude the employment of overly strict hierarchies. Anecdotally, there is a tendency to arrange concepts in a rigid hierarchical fashion synonymous with line and block charts. In practice, systems of this type are often accompanied by informal networks that are critical in achieving the functions the constituent components serve. As a result, an ontology patterned solely on a rigid hierarchy is incapable of addressing more complex and atypical circumstances that often arise in military situations. While some semblance of a hierarchy is required to provide structure to the problem domain, it should not be overly prescriptive.

There is no single authoritative way to express a problem domain, but there are better ways to capture reality in a meaningful structure. Adaptability, flexible and encompassing levels of abstraction, and avoidance of rigid hierarchies cumulatively offer a means of better characterizing complex domains.

D.   DEFINING THE RULES

The preceding section addressed the need to develop doctrine in a manner supporting both humans and machines. The means by which this may be accomplished is through semi-formal methods to logically characterize the relationships between entities. It is this logical underpinning that provides the critical element for allowing machines to reason about the domain. While the Semantic Web is often associated with meta-data, simply applying multiple labels to entities will only facilitate greater ease in searching for and retrieving data. To achieve the true promise of the Semantic Web, a mechanism is required to allow a given machine to consider an entity in the context of the entire domain.

While this may appear a bit vague, the rules are the means by which a domain is governed. To that end, a very small set of formal rules can be used to capture the essence of the IO domain. The example in the preceding chapters illustrated a means to characterize an IO resource as an aggregation of Platforms and Capabilities. Further, the domain was expanded to assert that these resources achieve effects in specified domains. With four specific rules, a machine understandable governing framework was established that captured the general essence of what IO seeks to accomplish. While the ontology offers a means of structuring the entities, well-defined rules provide a means of articulating their interaction.

E.   FUTURE RESEARCH

The objective of this thesis was to illustrate the means by which IO capabilities could be represented in an ontology suitable for the Semantic Web. This equates to a general methodology and is relatively narrow in scope. It is sufficient to illustrate a

means of visualizing the IO domain, but does not fully define it. In considering how this research could be expanded upon, several avenues become readily apparent:

1) Generate competing views of the IO domain. As previously stated, there are multiple ways of expressing any given problem domain, and this thesis has focused on one. It would be worthwhile to develop multiple views of the IO domain as a means of comparing and contrasting their respective merits. A single vision tends to reflect the biases and shortcomings of a single developer.

2) Expanded view of the existing domain. IO encompasses a broad range of topics, allowing for the significant expansion of the current artifacts. The ontology developed in this thesis has centered on IO resources and effects. While this captures the essence, the IO domain can be explored further. This could conceptually be achieved by adding in cultural variables, expanding the IO resource base to encompass supporting and related disciplines, or simply adding additional capabilities and platforms.

3) Expand the attributes of the existing elements. While somewhat similar to the preceding paragraph, this recommendation focuses on increasing the depth of the existing domain rather than breadth. More specifically, adding increasing detail to the platforms and capabilities introduced to more fully define their interactions with other entities.

4) More fully define the military applications of the Semantic Web. While it was illustrated that the IO domain can be expressed in a manner suitable for theSemantic Web, there has been limited discussion on the true military utility of this. A more detailed exploration of the military potential of the Semantic Web would offer further insight.

5) Development of Semantic Web applications for the IO domain. The longer term objective of machine understandable entities is to facilitate the swift and accurate completion of some task. The development of semantic applications more capable of reasoning about the entities being examined offers a means of achieving this.

Computers and their associated software have benefited mankind tremendously. To continue deriving benefit, certain obstacles need to be overcome. One of the recurring software challenges of our era is the seam between how humans perceive the world and how machines interpret our perceptions. Revisions to doctrine development procedures offer a means to mend the seam between domain expert and software developer. Ontologies offer the potential to frame the domain in such a context that the gap between man and machine is further narrowed. Well defined rules allow virtual entities to behave in a manner consistent with reality. The challenge is understood, the solution is ours to find.

APPENDIX A: IO PROBLEM DOMAIN EXPRESSED IN OWL

```
<rdf:RDF
xmlns:j.0="http://protege.stanford.edu/plugins/owl/protege#"
    xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
    xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
    xmlns:owl="http://www.w3.org/2002/07/owl#"
    xmlns="http://www.owl-ontologies.com/unnamed.owl#"
    xmlns:p1="http://www.owl-ontologies.com/assert.owl#"
  xml:base="http://www.owl-ontologies.com/unnamed.owl">
  <owl:Ontology rdf:about=""/>
  <owl:Class rdf:ID="Computer_Network_Exploitation">
    <owl:disjointWith>
      <owl:Class rdf:ID="Computer_Network_Attack"/>
    </owl:disjointWith>
    <owl:disjointWith>
      <owl:Class rdf:ID="Computer_Network_Defend"/>
    </owl:disjointWith>
    <rdfs:label      xml:lang="en">Computer      Network
Exploitation</rdfs:label>
    <rdfs:label xml:lang="en">CNE</rdfs:label>
    <rdfs:subClassOf>
      <owl:Class rdf:ID="Computer_Network_Operations"/>
    </rdfs:subClassOf>
    <rdfs:comment  xml:lang="en">Enabling  operations  and
intelligence collection capabilities
conducted  through  the  use  of  computer  networks  to  gather
data from target or adversary
automated  information  systems  or  networks.  Also  called  CNE.
(Approved for inclusion in
the next edition of JP 1-02.)</rdfs:comment>
  </owl:Class>
  <owl:Class rdf:ID="Electronic_Attack">
    <owl:disjointWith>
      <owl:Class rdf:ID="Electronic_Protect"/>
    </owl:disjointWith>
    <owl:disjointWith>
      <owl:Class rdf:ID="Electronic_Warfare_Support"/>
    </owl:disjointWith>
    <rdfs:comment  xml:lang="en">EA  includes:  1)  actions
taken to prevent or reduce an enemy's effective use of the
electromagnetic    spectrum,    such    as    jamming    and
electromagnetic deception, and 2) employment of weapons that
use  either  electromagnetic  or  directed  energy  as  their
```

```
primary  destructive  mechanism  (lasers,  radio  frequency
weapons, particle beams).</rdfs:comment>
    <rdfs:subClassOf>
      <owl:Class rdf:ID="Electronic_Warfare"/>
    </rdfs:subClassOf>
    <rdfs:label xml:lang="en">Electronic Attack</rdfs:label>
  </owl:Class>
  <owl:Class rdf:ID="Informational_Domain">
    <rdfs:subClassOf>
      <owl:Class rdf:ID="IO_Effects"/>
    </rdfs:subClassOf>
    <rdfs:comment xml:lang="en">The informational dimension
is  where  information  is  collected,  processed,  stored,
disseminated, displayed, and protected. It is the dimension
where the C2 of modern military forces is communicated, and
where  commander's  intent  is  conveyed.  It  consists  of  the
content  and  flow  of  information.  Consequently,  it  is  the
informational  dimension  that  must  be  protected.  (JP  3-
13)</rdfs:comment>
    <rdfs:label                    xml:lang="en">Informational
Dimension</rdfs:label>
    <owl:disjointWith>
      <owl:Class rdf:ID="Physical_Domain"/>
    </owl:disjointWith>
    <rdfs:label                      xml:lang="en">Information
Domain</rdfs:label>
    <owl:disjointWith>
      <owl:Class rdf:ID="Cognitive_Domain"/>
    </owl:disjointWith>
    <rdfs:label                    xml:lang="en">Informational
Domain</rdfs:label>
    <rdfs:label
rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
    >Informational Domain</rdfs:label>
    <rdfs:subClassOf>
      <owl:Restriction>
        <owl:someValuesFrom
rdf:resource="#Electronic_Attack"/>
        <owl:onProperty>
          <owl:ObjectProperty rdf:ID="impactedBy"/>
        </owl:onProperty>
      </owl:Restriction>
    </rdfs:subClassOf>
  </owl:Class>
  <owl:Class rdf:ID="Air">
    <owl:disjointWith>
```

```
        <owl:Class rdf:ID="Land"/>
      </owl:disjointWith>
      <owl:disjointWith>
        <owl:Class rdf:ID="Sea"/>
      </owl:disjointWith>
      <owl:disjointWith>
        <owl:Class rdf:ID="Space"/>
      </owl:disjointWith>
      <rdfs:subClassOf>
        <owl:Class rdf:ID="Platform"/>
      </rdfs:subClassOf>
      <rdfs:comment    xml:lang="en">Subclass    of    Platform.
Encompasses all aircraft that are associated with a specific
IO capability.</rdfs:comment>
    </owl:Class>
    <owl:Class rdf:about="#Electronic_Warfare">
      <rdfs:comment    xml:lang="en">Any    military    action
```
involving the use of electromagnetic and directed energy to
control the electromagnetic spectrum or to attack the enemy.
Also called EW.   The three major subdivisions within
electronic warfare are: electronic attack, electronic
protection, and electronic warfare support. a. electronic
attack. That division of electronic warfare involving the
use of electromagnetic energy, directed energy, or anti-
radiation weapons to attack personnel, facilities, or
equipment with the intent of degrading, neutralizing, or
destroying enemy combat capability and is considered a form
of fires. Also called EA. EA includes: 1) actions taken to
prevent or reduce an enemy's effective use of the
electromagnetic spectrum, such as jamming and
electromagnetic deception, and 2) employment of weapons that
use either electromagnetic or directed energy as their
primary destructive mechanism (lasers, radio frequency
weapons, particle beams). b. electronic protection. That
division of electronic warfare involving passive and active
means taken to protect personnel, facilities, and equipment
from any effects of friendly or enemy employment of
electronic warfare that degrade, neutralize, or destroy
friendly combat capability. Also called EP. c. electronic
warfare support. That division of electronic warfare
involving actions tasked by, or under direct control of, an
operational commander to search for, intercept, identify,
and locate or localize sources of intentional and
unintentional radiated electromagnetic energy for the
purpose of immediate threat recognition, targeting, planning
and conduct of future operations. Thus, electronic warfare

101

support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. See also directed energy; electromagnetic spectrum. (JP 1-02)</rdfs:comment>
    <rdfs:subClassOf>
      <owl:Class rdf:ID="Capability"/>
    </rdfs:subClassOf>
    <rdfs:label   xml:lang="en">Electronic Warfare</rdfs:label>
    <rdfs:label xml:lang="en">EW</rdfs:label>
    <owl:disjointWith>
      <owl:Class rdf:about="#Computer_Network_Operations"/>
    </owl:disjointWith>
    <owl:disjointWith>
      <owl:Class rdf:ID="Military_Deception"/>
    </owl:disjointWith>
    <owl:disjointWith>
      <owl:Class rdf:ID="Operations_Security"/>
    </owl:disjointWith>
    <owl:disjointWith>
      <owl:Class rdf:ID="Psychological_Operations"/>
    </owl:disjointWith>
  </owl:Class>
  <owl:Class rdf:about="#Computer_Network_Operations">
    <rdfs:subClassOf>
      <owl:Class rdf:about="#Capability"/>
    </rdfs:subClassOf>
    <owl:disjointWith rdf:resource="#Electronic_Warfare"/>
    <owl:disjointWith>
      <owl:Class rdf:about="#Military_Deception"/>
    </owl:disjointWith>
    <owl:disjointWith>
      <owl:Class rdf:about="#Operations_Security"/>
    </owl:disjointWith>
    <owl:disjointWith>
      <owl:Class rdf:about="#Psychological_Operations"/>
    </owl:disjointWith>
    <rdfs:comment   xml:lang="en">Comprised   of   computer network attack, computer network defense, and related computer network exploitation enabling operations. Also called CNO. (Approved for inclusion in the next edition of JP 1-02.)</rdfs:comment>

102

```
    <rdfs:label xml:lang="en">CNO</rdfs:label>
    <rdfs:label        xml:lang="en">Computer        Network
Operations</rdfs:label>
  </owl:Class>
  <owl:Class rdf:about="#Platform">
    <rdfs:subClassOf>
      <owl:Class rdf:ID="IO_Domain_Concept"/>
    </rdfs:subClassOf>
    <rdfs:subClassOf>
      <owl:Restriction>
        <owl:onProperty>
          <owl:ObjectProperty rdf:ID="hasCapability"/>
        </owl:onProperty>
        <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
        >1</owl:minCardinality>
      </owl:Restriction>
    </rdfs:subClassOf>
    <rdfs:comment xml:lang="en">Superclass  encompassing  the
core      platforms      associated      with      Information
Operations.</rdfs:comment>
    <owl:disjointWith>
      <owl:Class rdf:about="#IO_Effects"/>
    </owl:disjointWith>
    <owl:disjointWith>
      <owl:Class rdf:ID="Information_Operations_Resources"/>
    </owl:disjointWith>
    <owl:disjointWith>
      <owl:Class rdf:about="#IO_Domain_Concept"/>
    </owl:disjointWith>
    <owl:disjointWith>
      <owl:Class rdf:about="#Capability"/>
    </owl:disjointWith>
  </owl:Class>
  <owl:Class rdf:about="#Computer_Network_Attack">
    <rdfs:label        xml:lang="en">Computer        Network
Attack</rdfs:label>
    <rdfs:label xml:lang="en">CNA</rdfs:label>
    <owl:disjointWith>
      <owl:Class rdf:about="#Computer_Network_Defend"/>
    </owl:disjointWith>
    <owl:disjointWith
rdf:resource="#Computer_Network_Exploitation"/>
    <rdfs:comment  xml:lang="en">Actions  taken  through  the
use of computer networks to disrupt,
```

deny, degrade, or destroy information resident in computers and computer networks, or the
computers and networks themselves. Also called CNA. (This term and its definition modify
the existing term and its definition and are approved for inclusion in the next edition of JP
1-02.)</rdfs:comment>
    <rdfs:subClassOf
rdf:resource="#Computer_Network_Operations"/>
  </owl:Class>
  <owl:Class rdf:ID="EA6B">
    <rdfs:subClassOf rdf:resource="#Air"/>
    <rdfs:subClassOf>
      <owl:Restriction>
        <owl:someValuesFrom
rdf:resource="#Electronic_Warfare"/>
        <owl:onProperty rdf:resource="#hasCapability"/>
      </owl:Restriction>
    </rdfs:subClassOf>
    <rdfs:subClassOf>
      <owl:Restriction>
        <owl:onProperty rdf:resource="#hasCapability"/>
        <owl:someValuesFrom>
          <owl:Class rdf:ID="USQ113_v3"/>
        </owl:someValuesFrom>
      </owl:Restriction>
    </rdfs:subClassOf>
    <rdfs:label xml:lang="en">EA6B</rdfs:label>
    <rdfs:label xml:lang="en">EA-6B</rdfs:label>
    <rdfs:label xml:lang="en">Prowler</rdfs:label>
    <rdfs:label xml:lang="en">EA-6B Prowler</rdfs:label>
    <rdfs:comment xml:lang="en">The Northrop Grumman EA-6B Prowler is a carrier-capable, soft- and hard-kill SEAD and SIGINT aircraft that, as of 2005, was America's primary stand-off radar jamming platform. As such, the type is assigned to the US Navy (USN) and US Marine Corps (USMC) and there has been US Air Force (USAF) participation in those USN units that have been assigned an 'expeditionary' role. To maintain the Prowler's operational viability, the pool of available airframes has been consistently reworked, with a total of nine capability standards (designated as Standard (or Basic), EXpanded CAPability (EXCAP), Improved CAPability (ICAP) I, ICAP II Block 82, ICAP II Block 86, ICAP II Block 89, ICAP II Block 89A, ADVanced CAPability (ADVCAP) and ICAP III - see following and Programme history) having been identified since the aircraft's introduction into service in

September 1970. Of these, eight have been deployed operationally. As of 2005, the ICAP II Blocks 89 and 89A were the current service configurations, with the ICAP III being in development for a second quarter of US Fiscal Year (FY) 2005 Initial Operating Capability (IOC). (Janes, 12OCT07)</rdfs:comment>
  </owl:Class>
  <owl:Class rdf:about="#Cognitive_Domain">
    <rdfs:subClassOf>
      <owl:Restriction>
        <owl:someValuesFrom>
          <owl:Class rdf:about="#Psychological_Operations"/>
        </owl:someValuesFrom>
        <owl:onProperty rdf:resource="#impactedBy"/>
      </owl:Restriction>
    </rdfs:subClassOf>
    <rdfs:subClassOf>
      <owl:Class rdf:about="#IO_Effects"/>
    </rdfs:subClassOf>
    <rdfs:comment xml:lang="en">The cognitive dimension encompasses the mind of the decision maker and the target audience (TA). This is the dimension in which people think, perceive, visualize, and decide. It is the most important of the three dimensions. This dimension is also affected by a commander’s orders, training, and other personal motivations. Battles and campaigns can be lost in the cognitive dimension. Factors such as leadership, morale, unit cohesion, emotion, state of mind, level of training, experience, situational awareness, as well as public opinion, perceptions, media, public information, and rumors influence this dimension. (JP 3-13)</rdfs:comment>
    <rdfs:label   xml:lang="en">Cognitive Dimension</rdfs:label>
    <rdfs:label xml:lang="en">Cognitive Domain</rdfs:label>
    <owl:disjointWith>
      <owl:Class rdf:about="#Physical_Domain"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Informational_Domain"/>
  </owl:Class>
  <owl:Class rdf:about="#Physical_Domain">
    <rdfs:subClassOf>
      <owl:Class rdf:about="#IO_Effects"/>
    </rdfs:subClassOf>
    <owl:disjointWith rdf:resource="#Cognitive_Domain"/>
    <owl:disjointWith rdf:resource="#Informational_Domain"/>

```xml
    <rdfs:comment
rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
    >The physical dimension is composed of the command and
control (C2) systems, and supporting infrastructures that
enable individuals and organizations to conduct operations
across the air, land, sea, and space domains. It is also the
dimension where physical platforms and the communications
networks that connect them reside. This includes the means
of transmission, infrastructure, technologies, groups, and
populations. Comparatively, the elements of this dimension
are the easiest to measure, and consequently, combat power
has traditionally been measured primarily in this dimension.
(JP 3-13)</rdfs:comment>
  </owl:Class>
  <owl:Class rdf:about="#Sea">
    <rdfs:subClassOf rdf:resource="#Platform"/>
    <rdfs:comment    xml:lang="en">Subclass    of    Platform.
Encompasses all maritime assets that are associated with a
specific IO capability.</rdfs:comment>
    <owl:disjointWith rdf:resource="#Air"/>
    <owl:disjointWith>
      <owl:Class rdf:about="#Land"/>
    </owl:disjointWith>
    <owl:disjointWith>
      <owl:Class rdf:about="#Space"/>
    </owl:disjointWith>
  </owl:Class>
  <owl:Class rdf:about="#Military_Deception">
    <owl:disjointWith
rdf:resource="#Computer_Network_Operations"/>
    <owl:disjointWith rdf:resource="#Electronic_Warfare"/>
    <owl:disjointWith>
      <owl:Class rdf:about="#Operations_Security"/>
    </owl:disjointWith>
    <owl:disjointWith>
      <owl:Class rdf:about="#Psychological_Operations"/>
    </owl:disjointWith>
    <rdfs:subClassOf>
      <owl:Class rdf:about="#Capability"/>
    </rdfs:subClassOf>
    <rdfs:comment    xml:lang="en">Actions    executed    to
deliberately mislead adversary military decision makers as
to   friendly   military   capabilities,   intentions,   and
operations, thereby causing the adversary to take specific
actions   (or   inactions)   that   will   contribute   to   the
accomplishment of the
```

friendly forces mission. Also called MILDEC. See also deception. (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 3-58.)</rdfs:comment>
    <rdfs:label xml:lang="en">MILDEC</rdfs:label>
    <rdfs:label   xml:lang="en">Military Deception</rdfs:label>
  </owl:Class>
  <owl:Class rdf:about="#Electronic_Warfare_Support">
    <owl:disjointWith rdf:resource="#Electronic_Attack"/>
    <owl:disjointWith>
      <owl:Class rdf:about="#Electronic_Protect"/>
    </owl:disjointWith>
    <rdfs:subClassOf rdf:resource="#Electronic_Warfare"/>
    <rdfs:label   xml:lang="en">Electronic   Warfare Support</rdfs:label>
    <rdfs:label xml:lang="en">ES</rdfs:label>
    <rdfs:comment xml:lang="en">That division of electronic warfare involving actions tasked by, or underdirect control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES.</rdfs:comment>
  </owl:Class>
  <owl:Class rdf:about="#Space">
    <owl:disjointWith rdf:resource="#Air"/>
    <owl:disjointWith>
      <owl:Class rdf:about="#Land"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Sea"/>
    <rdfs:subClassOf rdf:resource="#Platform"/>
    <rdfs:comment   xml:lang="en">Subclass   of   Platform. Encompasses all space based assets that are associated with a specific IO capability.</rdfs:comment>
  </owl:Class>
  <owl:Class rdf:ID="Tactical_PSYOP_Battalion">
    <rdfs:label xml:lang="en">TPB</rdfs:label>
    <rdfs:label   xml:lang="en">Tactical   PSYOP Battalion</rdfs:label>
    <rdfs:subClassOf>
      <owl:Restriction>

```
        <owl:someValuesFrom>
          <owl:Class rdf:ID="Leaflet_Dissemination"/>
        </owl:someValuesFrom>
        <owl:onProperty rdf:resource="#hasCapability"/>
      </owl:Restriction>
    </rdfs:subClassOf>
    <rdfs:subClassOf>
      <owl:Class rdf:about="#Land"/>
    </rdfs:subClassOf>
    <rdfs:comment xml:lang="en">Concrete instance of a land
platform associated with IO.  Tactical PSYOP Battalions
(TPB) provide tactical PSYOP support to corps level units
and below and select special operations and conventional
task forces at Army-level equivalent-sized units. The TPB
develops, produces, and disseminates tactical products
within the guidance (themes, objectives, and foreign TAs)
assigned by the JPOTF and authorized by the product approval
authority (combatant commander or subordinate JFC). The
TPBâ€™s capabilities include dissemination of PSYOP products
by loudspeaker message, leaflet, handbill, and face-to-face
communications.</rdfs:comment>
  </owl:Class>
  <owl:Class rdf:about="#Computer_Network_Defend">
    <owl:disjointWith
rdf:resource="#Computer_Network_Attack"/>
    <owl:disjointWith
rdf:resource="#Computer_Network_Exploitation"/>
    <rdfs:comment xml:lang="en">Actions taken through the
use of computer networks to protect,
monitor, analyze, detect and respond to unauthorized
activity within Department of Defense
information systems and computer networks. Also called CND.
(This term and its definition modify the existing term and
its definition and are approved for inclusion in the next
edition of JP 1-
02.)</rdfs:comment>
    <rdfs:label        xml:lang="en">Computer       Network
Defend</rdfs:label>
    <rdfs:label xml:lang="en">CND</rdfs:label>
    <rdfs:subClassOf
rdf:resource="#Computer_Network_Operations"/>
  </owl:Class>
  <owl:Class rdf:about="#Psychological_Operations">
    <owl:disjointWith
rdf:resource="#Computer_Network_Operations"/>
    <owl:disjointWith rdf:resource="#Electronic_Warfare"/>
```

```
    <owl:disjointWith rdf:resource="#Military_Deception"/>
    <owl:disjointWith>
      <owl:Class rdf:about="#Operations_Security"/>
    </owl:disjointWith>
    <rdfs:label xml:lang="en">PSYOP</rdfs:label>
    <rdfs:label                    xml:lang="en">Psychological
Operations</rdfs:label>
    <rdfs:comment xml:lang="en">Planned operations to convey
selected information and indicators to foreign audiences to
influence their emotions, motives, objective reasoning, and
ultimately    the    behavior    of    foreign    governments,
organizations, groups, and individuals. The purpose
of  psychological  operations  is  to  induce  or  reinforce
foreign    attitudes    and    behavior    favorable    to    the
originatorâ€™s   objectives.   Also   called   PSYOP.   (JP   1-
02)</rdfs:comment>
    <rdfs:subClassOf>
      <owl:Class rdf:about="#Capability"/>
    </rdfs:subClassOf>
  </owl:Class>
  <owl:Class rdf:about="#Capability">
    <owl:disjointWith>
      <owl:Class rdf:about="#IO_Effects"/>
    </owl:disjointWith>
    <owl:disjointWith>
      <owl:Class
rdf:about="#Information_Operations_Resources"/>
    </owl:disjointWith>
    <owl:disjointWith>
      <owl:Class rdf:about="#IO_Domain_Concept"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Platform"/>
    <rdfs:subClassOf>
      <owl:Class rdf:about="#IO_Domain_Concept"/>
    </rdfs:subClassOf>
    <rdfs:subClassOf>
      <owl:Restriction>
        <owl:onProperty>
          <owl:ObjectProperty rdf:ID="hasPlatform"/>
        </owl:onProperty>
        <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
        >1</owl:minCardinality>
      </owl:Restriction>
    </rdfs:subClassOf>
```

```
    <rdfs:comment xml:lang="en">Superclass encompassing the
core capabilities of Information Operations.</rdfs:comment>
  </owl:Class>
  <owl:Class rdf:about="#USQ113_v3">
    <rdfs:label xml:lang="en">USQ 113</rdfs:label>
    <rdfs:label xml:lang="en">AN/USQ 113</rdfs:label>
    <rdfs:label    xml:lang="en">AN/USQ-113    communications
jammer</rdfs:label>
    <rdfs:label xml:lang="en">USQ-113</rdfs:label>
    <rdfs:label xml:lang="en">USQ-113(V)3</rdfs:label>
    <rdfs:comment xml:lang="en">Understood to have also been
known as USQ-113(V)2 Phase III, USN sources describe the
USQ-113(V)3   as   enhancing   the   USQ-113(V)2   Phase   I
architecture   via   the   introduction   of   AN/ARC-210(V)
acquisition and analysis receivers, a new system controller,
a new operator control format (that matches the equipment's
laptop   computer's   display   format),   signal   recognition
algorithms   (planned   as   including   amplitude   modulation,
on/off keyed, frequency/phase modulated and frequency shift
keying) and improved reliability measures. As installed in
the EA-6B, USQ-113(V)3 includes a dorsally mounted reception
blade antenna (carried over from the USQ-113(V)2 Phase I
configuration), a ventrally mounted rectangular transmission
aerial (USQ-113(V)2 Phase I), a rear fuselage-mounted high
power   amplifier   (USQ-113(V)2   Phase   I),   a   rear   fuselage-
mounted   system   control   unit   (new   USQ-113(V)3   component),
rear   fuselage-mounted   ARC-210(V)   block   converters   (USQ-
113(V)3), a cockpit laptop interface (USQ-113(V)3) and an
operator control panel (USQ-113(V)3). As of November 2001,
the system's planned frequency coverage was 100 to 500 MHz
in transmit mode and 20 to 2,500 MHz in receive mode. In
terms   of   development,   three   engineering   and   development
manufacturing (V)3 preproduction examples were included in
the   cited   September   1996   USQ-113(V)2   to   (V)3   upgrade
contract. On 31 August 1998, BAE Systems was awarded a then
year USD12.9 million production contract covering the supply
of 33 USQ-113(V)3 (then known as the USQ-113(V)2 Phase III)
systems and two 'improved' operator panels that are all
understood to have been delivered during the first and third
quarters   of   US   FY2000.   Four   additional   USQ-113(V)3
equipments (for use by the USN Reserve) were procured as a
then year USD1.7 million modification to the cited August
1998   (V)3   production   contract   that   was   awarded   to   BAE
Systems   on   30   August   2000.   (Janes,   31   August
2007)</rdfs:comment>
    <rdfs:subClassOf rdf:resource="#Electronic_Attack"/>
```

```xml
      <rdfs:subClassOf>
        <owl:Restriction>
          <owl:onProperty rdf:resource="#hasPlatform"/>
          <owl:someValuesFrom rdf:resource="#EA6B"/>
        </owl:Restriction>
      </rdfs:subClassOf>
    </owl:Class>
    <owl:Class rdf:about="#Information_Operations_Resources">
      <rdfs:comment xml:lang="en">Information Operations are
the integrated employment of the core capabilities of
electronic warfare, computer network operations,
psychological operations, military deception, and operations
security, in concert with specified supporting and related
capabilities, to influence, disrupt, corrupt or usurp
adversarial human and automated decision making while
protecting our own.  Joint Publication 1-02.</rdfs:comment>
      <owl:disjointWith>
        <owl:Class rdf:about="#IO_Domain_Concept"/>
      </owl:disjointWith>
      <rdfs:label                    xml:lang="en">Information
Warfare</rdfs:label>
      <rdfs:label xml:lang="en">IO</rdfs:label>
      <rdfs:subClassOf>
        <owl:Restriction>
          <owl:onProperty rdf:resource="#hasCapability"/>
          <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
          >1</owl:minCardinality>
        </owl:Restriction>
      </rdfs:subClassOf>
      <owl:disjointWith rdf:resource="#Platform"/>
      <owl:disjointWith>
        <owl:Class rdf:about="#IO_Effects"/>
      </owl:disjointWith>
      <rdfs:label                    xml:lang="en">Information
Operations</rdfs:label>
      <rdfs:comment   xml:lang="en">As   structured   in   this
hierarchy, IInformation Operations Resources are defined by
the combination of a platform that operates in a given
medium or mediums combined with the specific IO capability
resident on it.</rdfs:comment>
      <rdfs:subClassOf>
        <owl:Restriction>
          <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
          >1</owl:minCardinality>
```

```
      <owl:onProperty rdf:resource="#hasPlatform"/>
    </owl:Restriction>
  </rdfs:subClassOf>
  <owl:disjointWith rdf:resource="#Capability"/>
  <rdfs:subClassOf>
    <owl:Class rdf:about="#IO_Domain_Concept"/>
  </rdfs:subClassOf>
  <rdfs:subClassOf>
    <owl:Class>
      <owl:intersectionOf rdf:parseType="Collection">
        <owl:Class rdf:about="#Platform"/>
        <owl:Class rdf:about="#Capability"/>
      </owl:intersectionOf>
    </owl:Class>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#Electronic_Protect">
  <rdfs:label                      xml:lang="en">Electronic
Protect</rdfs:label>
  <rdfs:label xml:lang="en">EP</rdfs:label>
  <owl:disjointWith rdf:resource="#Electronic_Attack"/>
  <owl:disjointWith
rdf:resource="#Electronic_Warfare_Support"/>
  <rdfs:subClassOf rdf:resource="#Electronic_Warfare"/>
  <rdfs:comment xml:lang="en">That division of electronic
warfare involving passive and active means taken to protect
personnel, facilities, and equipment from any effects of
friendly or enemy employment of electronic warfare that
degrade, neutralize, or destroy friendly combat capability.
Also called EP.</rdfs:comment>
</owl:Class>
<owl:Class rdf:about="#Operations_Security">
  <rdfs:label                      xml:lang="en">Operations
Security</rdfs:label>
  <rdfs:label xml:lang="en">OPSEC</rdfs:label>
  <rdfs:subClassOf rdf:resource="#Capability"/>
  <owl:disjointWith
rdf:resource="#Computer_Network_Operations"/>
  <owl:disjointWith rdf:resource="#Electronic_Warfare"/>
  <owl:disjointWith rdf:resource="#Military_Deception"/>
  <owl:disjointWith
rdf:resource="#Psychological_Operations"/>
  <rdfs:comment xml:lang="en">A process of identifying
critical information and subsequently analyzing friendly
actions attendant to military operations and other
activities to: a. identify those actions that can be
```

observed by adversary intelligence systems; b. determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (JP 1-02)</rdfs:comment>
  </owl:Class>
  <owl:Class rdf:about="#Land">
    <rdfs:subClassOf rdf:resource="#Platform"/>
    <owl:disjointWith rdf:resource="#Air"/>
    <owl:disjointWith rdf:resource="#Sea"/>
    <owl:disjointWith rdf:resource="#Space"/>
    <rdfs:comment   xml:lang="en">Subclass   of   Platform. Encompasses all land based entities that are associated with a specific IO capability.</rdfs:comment>
  </owl:Class>
  <owl:Class rdf:about="#Leaflet_Dissemination">
    <rdfs:label   xml:lang="en">Leaflet Operations</rdfs:label>
    <rdfs:comment
rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
    >Leaflet propaganda is a form of psychological warfare that militaries use in foreign conflict to alter the behavior of people in enemy-controlled territory. Airplanes have been instrumental in the deliverance of leaflets over enemy territories. In conjunction with air strikes, this method has been successful in influencing the enemyâ€™s way of thinking. In particular, persuading them to surrender, abandon their positions, and to cease fighting. Humanitarian air missions, in cooperation with leaflet propaganda, are also successful in turning civilians against enemy leadership while preparing them for the arrival of enemy troops.</rdfs:comment>
    <rdfs:label xml:lang="en">Handbills</rdfs:label>
    <rdfs:label   xml:lang="en">Leaflet Dissemination</rdfs:label>
    <rdfs:subClassOf>
      <owl:Restriction>
        <owl:someValuesFrom
rdf:resource="#Tactical_PSYOP_Battalion"/>
        <owl:onProperty rdf:resource="#hasPlatform"/>
      </owl:Restriction>
    </rdfs:subClassOf>
    <rdfs:label xml:lang="en">Leaflet Container</rdfs:label>

```
    <rdfs:label xml:lang="en">Leaflet</rdfs:label>
    <rdfs:label xml:lang="en">Leaflet Rolls</rdfs:label>
    <rdfs:label xml:lang="en">Leaflet Airdrop</rdfs:label>
    <rdfs:label xml:lang="en">Leaflet Drop</rdfs:label>
    <rdfs:subClassOf
rdf:resource="#Psychological_Operations"/>
    <rdfs:label xml:lang="en">Leaflet Bombs</rdfs:label>
  </owl:Class>
  <owl:Class rdf:about="#IO_Domain_Concept">
    <rdfs:comment    xml:lang="en">Information    Operations,
Capability,  and  Platform  each  reside  under  the  broader
category of IO Domain Concept.  This was established as such
because  a  unifying  concept  beyond  strictly  Information
Operations was required.  While IO can be considered as the
aggregation  of  capability  and  platform,  it  cannot  exist
without both.   The nature of this dependency prompted the
need    for    an    alternative    means    to    encompass    the
domain.</rdfs:comment>
    <owl:disjointWith rdf:resource="#Capability"/>
    <owl:disjointWith rdf:resource="#Platform"/>
    <owl:disjointWith
rdf:resource="#Information_Operations_Resources"/>
  </owl:Class>
  <owl:Class rdf:about="#IO_Effects">
    <owl:disjointWith rdf:resource="#Platform"/>
    <owl:disjointWith
rdf:resource="#Information_Operations_Resources"/>
    <owl:disjointWith rdf:resource="#Capability"/>
    <rdfs:comment
rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
    >The  physical  or  behavioral  state  of  a  system  that
results from an action, a set of
actions,  or  another  effect. 2.  The  result,  outcome,  or
consequence of an action. 3. A change
to  a  condition,  behavior,  or  degree  of  freedom. (JP  3-
0)</rdfs:comment>
    <rdfs:subClassOf>
      <owl:Restriction>
        <owl:onProperty rdf:resource="#impactedBy"/>
        <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
        >1</owl:minCardinality>
        <owl:valuesFrom
rdf:resource="#Information_Operations_Resources"/>
      </owl:Restriction>
    </rdfs:subClassOf>
```

114

```
    <rdfs:subClassOf rdf:resource="#IO_Domain_Concept"/>
  </owl:Class>
  <owl:DatatypeProperty
rdf:ID="IO_REV2_Baseline_30MAR08_DatatypeProperty_6"/>
  <j.0:PAL-CONSTRAINT rdf:ID="IO_TEST_Instance_2">
    <rdfs:label
rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
    >IO TEST_Instance_2</rdfs:label>
  </j.0:PAL-CONSTRAINT>
  <j.0:PAL-CONSTRAINT rdf:ID="IO_TEST_Instance_1">
    <rdfs:label
rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
    >IO TEST_Instance_1</rdfs:label>
  </j.0:PAL-CONSTRAINT>
  <j.0:PAL-CONSTRAINT rdf:ID="IO_TEST_Instance_0">
    <rdfs:label
rdf:datatype="http://www.w3.org/2001/XMLSchema#string"
    >IO TEST_Instance_0</rdfs:label>
  </j.0:PAL-CONSTRAINT>
  <Information_Operations_Resources
rdf:ID="Information_Operations_1"/>
</rdf:RDF>

<!-- Created with Protege (with OWL Plugin 3.3, Build 418)
http://protege.stanford.edu -->
```

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B:　　　　IO PROBLEM DOMAIN EXPRESSED IN JAVA SCHEMA

```java
/* CVS $Id: $ */
package ;
import com.hp.hpl.jena.rdf.model.*;
import com.hp.hpl.jena.ontology.*;
/**
 *         Vocabulary          definitions          from
file:/C:/Program%20Files/Protege_3.3/schemagen-temp.owl
 * @author Auto-generated by schemagen on 30 Mar 2008 18:00
 */
public class  {
    /** <p>The ontology model that holds the vocabulary
terms</p> */
    private       static       OntModel       m_model       =
ModelFactory.createOntologyModel( OntModelSpec.OWL_MEM, null
);

    /** <p>The namespace of the vocabulary as a string</p>
*/
    public   static   final   String   NS   =   "http://www.owl-
ontologies.com/unnamed.owl#";

    /** <p>The namespace of the vocabulary as a string</p>
     *  @see #NS */
    public static String getURI() {return NS;}

    /** <p>The namespace of the vocabulary as a resource</p>
*/
    public     static     final     Resource     NAMESPACE     =
m_model.createResource( NS );

    public   static   final   ObjectProperty   hasPlatform   =
m_model.createObjectProperty(                "http://www.owl-
ontologies.com/unnamed.owl#hasPlatform" );

    public   static   final   ObjectProperty   hasCapability   =
m_model.createObjectProperty(                "http://www.owl-
ontologies.com/unnamed.owl#hasCapability" );

    public   static   final   ObjectProperty   impactedBy   =
m_model.createObjectProperty(                "http://www.owl-
ontologies.com/unnamed.owl#impactedBy" );
```

117

```java
    public      static      final      DatatypeProperty
IO_REV2_Baseline_30MAR08_DatatypeProperty_6                =
m_model.createDatatypeProperty(         "http://www.owl-
ontologies.com/unnamed.owl#IO_REV2_Baseline_30MAR08_Datatype
Property_6" );

    /**   <p>Information   Operations   are   the   integrated
employment of the core capabilities
    *   of electronic warfare, computer network operations,
psychological operations,
    *    military  deception,  and  operations  security,  in
concert with specified supporting
    *    and  related  capabilities,  to  influence,  disrupt,
corrupt or usurp adversarial
    *   human and automated decision making while protecting
our own. Joint Publication
    *    1-02.As  structured  in  this  hierarchy,  IInformation
Operations Resources are
    *    defined  by  the  combination  of  a  platform  that
operates in a given medium or
    *    mediums  combined  with  the  specific  IO  capability
resident on it.</p>
    */
    public           static           final           OntClass
Information_Operations_Resources   =   m_model.createClass(
"http://www.owl-
ontologies.com/unnamed.owl#Information_Operations_Resources"
);

    /** <p>Planned operations to convey selected information
and indicators to foreign
    *    audiences  to  influence  their  emotions,  motives,
objective reasoning, and ultimately
    *   the behavior of foreign governments, organizations,
groups, and individuals.
    *   The purpose of psychological operations is to induce
or reinforce foreign
    *   attitudes and behavior favorable to the originator's
objectives. Also called
    *   PSYOP. (JP 1-02)</p>
    */
    public static final OntClass Psychological_Operations =
m_model.createClass(                        "http://www.owl-
ontologies.com/unnamed.owl#Psychological_Operations" );
```

```java
    /** <p>Subclass of Platform. Encompasses all space based
assets that are associated
     *  with a specific IO capability.</p>
     */
    public    static    final    OntClass    Space    =
m_model.createClass(                            "http://www.owl-
ontologies.com/unnamed.owl#Space" );

    /** <p>Leaflet propaganda is a form of psychological
warfare that militaries use
     *  in foreign conflict to alter the behavior of people
in enemy-controlled territory.
     *  Airplanes have been instrumental in the deliverance
of leaflets over enemy
     *  territories. In conjunction with air strikes, this
method has been successful
     *  in influencing the enemy's way of thinking. In
particular, persuading them
     *  to surrender, abandon their positions, and to cease
fighting. Humanitarian
     *  air missions, in cooperation with leaflet
propaganda, are also successful
     *  in turning civilians against enemy leadership while
preparing them for the
     *  arrival of enemy troops.</p>
     */
    public  static  final  OntClass  Leaflet_Dissemination  =
m_model.createClass(                            "http://www.owl-
ontologies.com/unnamed.owl#Leaflet_Dissemination" );

    /** <p>Superclass encompassing the core capabilities of
Information Operations.</p> */
    public    static    final    OntClass    Capability    =
m_model.createClass(                            "http://www.owl-
ontologies.com/unnamed.owl#Capability" );

    /** <p>Enabling operations and intelligence collection
capabilities conducted through
     *  the use of computer networks to gather data from
target or adversary automated
     *  information systems or networks. Also called CNE.
(Approved for inclusion
     *  in the next edition of JP 1-02.)</p>
     */
    public          static          final          OntClass
Computer_Network_Exploitation    =    m_model.createClass(
```

```java
"http://www.owl-
ontologies.com/unnamed.owl#Computer_Network_Exploitation" );

    /** <p>EA includes: 1) actions taken to prevent or
reduce an enemy's effective use
     *  of the electromagnetic spectrum, such as jamming and
electromagnetic deception,
     *   and 2) employment of weapons that use either
electromagnetic or directed energy
     *   as their primary destructive mechanism (lasers,
radio frequency weapons, particle
     *  beams).</p>
     */
    public  static  final  OntClass  Electronic_Attack  =
m_model.createClass(                     "http://www.owl-
ontologies.com/unnamed.owl#Electronic_Attack" );

    /** <p>A process of identifying critical information and
subsequently analyzing friendly
     *   actions attendant to military operations and other
activities to: a. identify
     *   those actions that can be observed by adversary
intelligence systems; b. determine
     *   indicators that hostile intelligence systems might
obtain that could be interpreted
     *  or pieced together to derive critical information in
time to be useful to
     *  adversaries; and c. select and execute measures that
eliminate or reduce to
     *   an acceptable level the vulnerabilities of friendly
actions to adversary exploitation.
     *  Also called OPSEC. (JP 1-02)</p>
     */
    public  static  final  OntClass  Operations_Security  =
m_model.createClass(                     "http://www.owl-
ontologies.com/unnamed.owl#Operations_Security" );

    /**  <p>Superclass  encompassing  the  core  platforms
associated with Information Operations.</p> */
    public    static    final    OntClass    Platform    =
m_model.createClass(                     "http://www.owl-
ontologies.com/unnamed.owl#Platform" );

    /** <p>The physical or behavioral state of a system that
results from an action,
```

```java
     *  a set of actions, or another effect. 2. The result,
outcome, or consequence
     *  of an action. 3. A change to a condition, behavior,
or degree of freedom.
     *  (JP 3-0)</p>
     */
    public   static   final   OntClass   IO_Effects   =
m_model.createClass(                          "http://www.owl-
ontologies.com/unnamed.owl#IO_Effects" );

    /** <p>Subclass of Platform. Encompasses all maritime
assets that are associated
     *  with a specific IO capability.</p>
     */
    public static final OntClass Sea = m_model.createClass(
"http://www.owl-ontologies.com/unnamed.owl#Sea" );

    /** <p>The informational dimension is where information
is collected, processed,
     *  stored, disseminated, displayed, and protected. It
is the dimension where
     *  the C2 of modern military forces is communicated,
and where commander's intent
     *  is conveyed. It consists of the content and flow of
information. Consequently,
     *  it is the informational dimension that must be
protected. (JP 3-13)</p>
     */
    public   static   final   OntClass   Informational_Domain   =
m_model.createClass(                          "http://www.owl-
ontologies.com/unnamed.owl#Informational_Domain" );

    /** <p>Subclass of Platform. Encompasses all land based
entities that are associated
     *  with a specific IO capability.</p>
     */
    public static final OntClass Land = m_model.createClass(
"http://www.owl-ontologies.com/unnamed.owl#Land" );

    /** <p>The Northrop Grumman EA-6B Prowler is a carrier-
capable, soft- and hard-kill
     *  SEAD and SIGINT aircraft that, as of 2005, was
America's primary stand-off
     *  radar jamming platform. As such, the type is
assigned to the US Navy (USN)
```

*   and US Marine Corps (USMC) and there has been US Air
Force (USAF) participation
     *   in those USN units that have been assigned an
'expeditionary' role. To maintain
     *   the Prowler's operational viability, the pool of
available airframes has been
     *   consistently reworked, with a total of nine
capability standards (designated
     *   as Standard (or Basic), EXpanded CAPability (EXCAP),
Improved CAPability (ICAP)
     *   I, ICAP II Block 82, ICAP II Block 86, ICAP II Block
89, ICAP II Block 89A,
     *   ADVanced CAPability (ADVCAP) and ICAP III - see
following and Programme history)
     *   having been identified since the aircraft's
introduction into service in September
     *   1970. Of these, eight have been deployed
operationally. As of 2005, the ICAP
     *   II Blocks 89 and 89A were the current service
configurations, with the ICAP
     *   III being in development for a second quarter of US
Fiscal Year (FY) 2005
     *   Initial Operating Capability (IOC). (Janes,
12OCT07)</p>
     */
    public static final OntClass EA6B = m_model.createClass(
"http://www.owl-ontologies.com/unnamed.owl#EA6B");

    /** <p>Understood to have also been known as USQ-113(V)2
Phase III, USN sources describe
     *   the USQ-113(V)3 as enhancing the USQ-113(V)2 Phase I
architecture via the
     *   introduction of AN/ARC-210(V) acquisition and
analysis receivers, a new system
     *   controller, a new operator control format (that
matches the equipment's laptop
     *   computer's display format), signal recognition
algorithms (planned as including
     *   amplitude modulation, on/off keyed, frequency/phase
modulated and frequency
     *   shift keying) and improved reliability measures. As
installed in the EA-6B,
     *   USQ-113(V)3 includes a dorsally mounted reception
blade antenna (carried over
     *   from the USQ-113(V)2 Phase I configuration), a
ventrally mounted rectangular

122

```
     *    transmission aerial (USQ-113(V)2 Phase I), a rear
fuselage-mounted high power
     *    amplifier (USQ-113(V)2 Phase I), a rear fuselage-
mounted system control unit
     *    (new USQ-113(V)3 component), rear fuselage-mounted
ARC-210(V) block converters
     *    (USQ-113(V)3), a cockpit laptop interface (USQ-
113(V)3) and an operator control
     *    panel (USQ-113(V)3). As of November 2001, the
system's planned frequency coverage
     *    was 100 to 500 MHz in transmit mode and 20 to 2,500
MHz in receive mode. In
     *    terms of development, three engineering and
development manufacturing (V)3
     *    preproduction examples were included in the cited
September 1996 USQ-113(V)2
     *    to (V)3 upgrade contract. On 31 August 1998, BAE
Systems was awarded a then
     *    year USD12.9 million production contract covering
the supply of 33 USQ-113(V)3
     *    (then known as the USQ-113(V)2 Phase III) systems
and two 'improved' operator
     *    panels that are all understood to have been
delivered during the first and
     *    third quarters of US FY2000. Four additional USQ-
113(V)3 equipments (for use
     *    by the USN Reserve) were procured as a then year
USD1.7 million modification
     *    to the cited August 1998 (V)3 production contract
that was awarded to BAE
     *    Systems on 30 August 2000. (Janes, 31 August
2007)</p>
     */
    public    static    final    OntClass    USQ113_v3    =
m_model.createClass(                        "http://www.owl-
ontologies.com/unnamed.owl#USQ113_v3" );


    /**   <p>Actions    executed    to    deliberately    mislead
adversary military decision makers
     *    as to friendly military capabilities, intentions,
and operations, thereby
     *    causing the adversary to take specific actions (or
inactions) that will contribute
     *    to the accomplishment of the friendly forces
mission. Also called MILDEC.
```

```
    *    See also deception. (This term and its definition
are provided for information
    *    and are proposed for inclusion in the next edition
of JP 1-02 by JP 3-58.)</p>
    */
    public static final OntClass Military_Deception =
m_model.createClass(                          "http://www.owl-
ontologies.com/unnamed.owl#Military_Deception" );


    /**  <p>Any  military  action  involving  the  use  of
electromagnetic and directed energy
    *   to control the electromagnetic spectrum or to attack
the enemy. Also called
    *    EW. The three major subdivisions within electronic
warfare are: electronic
    *     attack,   electronic   protection,   and   electronic
warfare support. a. electronic
    *     attack.   That   division   of   electronic   warfare
involving the use of electromagnetic
    *   energy, directed energy, or antiradiation weapons to
attack personnel, facilities,
    *     or   equipment   with   the   intent   of   degrading,
neutralizing, or destroying enemy
    *   combat capability and is considered a form of fires.
Also called EA. EA includes:
    *    1) actions taken to prevent or reduce an enemy's
effective use of the electromagnetic
    *     spectrum,   such   as   jamming   and   electromagnetic
deception, and 2) employment
    *     of   weapons   that   use   either   electromagnetic   or
directed energy as their primary
    *     destructive   mechanism   (lasers,   radio   frequency
weapons, particle beams). b.
    *   electronic protection. That division of electronic
warfare involving passive
    *     and   active   means   taken   to   protect   personnel,
facilities, and equipment from
    *    any effects of friendly or enemy employment of
electronic warfare that degrade,
    *   neutralize, or destroy friendly combat capability.
Also called EP. c. electronic
    *   warfare support. That division of electronic warfare
involving actions tasked
    *     by,   or   under   direct   control   of,   an   operational
commander to search for, intercept,
```

```
     *      identify,  and  locate  or  localize  sources  of
intentional and unintentional
     *   radiated electromagnetic energy for the purpose of
immediate threat recognition,
     *       targeting,  planning  and  conduct  of  future
operations. Thus, electronic warfare
     *   support provides information required for decisions
involving electronic warfare
     *   operations and other tactical actions such as threat
avoidance, targeting,
     *    and  homing.  Also  called  ES.  Electronic  warfare
support data can be used to
     *   produce signals intelligence, provide targeting for
electronic or destructive
     *      attack,  and  produce  measurement  and  signature
intelligence. See also directed
     *   energy; electromagnetic spectrum. (JP 1-02)</p>
     */
    public   static   final   OntClass   Electronic_Warfare   =
m_model.createClass(                          "http://www.owl-
ontologies.com/unnamed.owl#Electronic_Warfare" );

    /** <p>That  division  of  electronic  warfare  involving
actions tasked by, or underdirect
     *   control of, an operational commander to search for,
intercept, identify, and
     *    locate  or  localize  sources  of  intentional  and
unintentional radiated electromagnetic
     *     energy  for  the  purpose  of  immediate  threat
recognition, targeting, planning
     *   and conduct of future operations. Thus, electronic
warfare support provides
     *      information  required  for  decisions  involving
electronic warfare operations
     *   and other tactical actions such as threat avoidance,
targeting, and homing.
     *   Also called ES.</p>
     */
    public static final OntClass Electronic_Warfare_Support
=        m_model.createClass(            "http://www.owl-
ontologies.com/unnamed.owl#Electronic_Warfare_Support" );

    /** <p>Subclass  of  Platform.  Encompasses  all  aircraft
that are associated with a
     *   specific IO capability.</p>
     */
```

```java
    public static final OntClass Air = m_model.createClass(
"http://www.owl-ontologies.com/unnamed.owl#Air" );

    /**  <p>Actions  taken  through  the  use  of  computer
networks to protect, monitor, analyze,
    *   detect and respond to unauthorized activity within
Department of Defense information
    *    systems  and  computer  networks.  Also  called  CND.
(This term and its definition
    *   modify the existing term and its definition and are
approved for inclusion
    *   in the next edition of JP 1- 02.)</p>
    */
    public  static  final  OntClass Computer_Network_Defend =
m_model.createClass(                            "http://www.owl-
ontologies.com/unnamed.owl#Computer_Network_Defend" );

    /**  <p>That  division  of  electronic  warfare  involving
passive and active means taken
    *   to protect personnel, facilities, and equipment from
any effects of friendly
    *    or  enemy  employment  of  electronic  warfare  that
degrade, neutralize, or destroy
    *   friendly combat capability. Also called EP.</p>
    */
    public   static   final   OntClass   Electronic_Protect   =
m_model.createClass(                            "http://www.owl-
ontologies.com/unnamed.owl#Electronic_Protect" );

    /** <p>The physical dimension is composed of the command
and control (C2) systems,
    *    and   supporting   infrastructures   that   enable
individuals and organizations to
    *   conduct operations across the air, land, sea, and
space domains. It is also
    *    the  dimension  where  physical  platforms  and  the
communications networks that
    *    connect  them  reside.  This  includes  the  means  of
transmission, infrastructure,
    *      technologies,    groups,    and    populations.
Comparatively, the elements of this
    *     dimension   are   the   easiest   to   measure,   and
consequently, combat power has traditionally
    *   been measured primarily in this dimension. (JP 3-
13)</p>
    */
```

```java
    public    static    final    OntClass    Physical_Domain    =
m_model.createClass(                                "http://www.owl-
ontologies.com/unnamed.owl#Physical_Domain" );


    /** <p>Information Operations, Capability, and Platform
each reside under the broader
     *  category of IO Domain Concept. This was established
as such because a unifying
     *  concept beyond strictly Information Operations was
required. While IO can
     *  be considered as the aggregation of capability and
platform, it cannot exist
     *  without both. The nature of this dependency prompted
the need for an alternative
     *  means to encompass the domain.</p>
     */
    public    static    final    OntClass    IO_Domain_Concept    =
m_model.createClass(                                "http://www.owl-
ontologies.com/unnamed.owl#IO_Domain_Concept" );


    /** <p>Concrete instance of a land platform associated
with IO. Tactical PSYOP Battalions
     *  (TPB) provide tactical PSYOP support to corps level
units and below and select
     *  special operations and conventional task forces at
Army-level equivalent-sized
     *  units. The TPB develops, produces, and disseminates
tactical products within
     *  the guidance (themes, objectives, and foreign TAs)
assigned by the JPOTF and
     *   authorized  by  the  product  approval  authority
(combatant commander or subordinate
     *  JFC). The TPB's capabilities include dissemination
of PSYOP products by loudspeaker
     *   message,  leaflet,  handbill,  and  face-to-face
communications.</p>
     */
    public static final OntClass Tactical_PSYOP_Battalion =
m_model.createClass(                                "http://www.owl-
ontologies.com/unnamed.owl#Tactical_PSYOP_Battalion" );


    /** <p>The cognitive dimension encompasses the mind of
the decision maker and the
     *  target audience (TA). This is the dimension in which
people think, perceive,
```

```java
    *   visualize, and decide. It is the most important of
the three dimensions. This
    *   dimension is also affected by a commander's orders,
training, and other personal
    *   motivations. Battles and campaigns can be lost in
the cognitive dimension.
    *   Factors such as leadership, morale, unit cohesion,
emotion, state of mind,
    *     level   of   training,   experience,   situational
awareness, as well as public opinion,
    *   perceptions, media, public information, and rumors
influence this dimension.
    *   (JP 3-13)</p>
    */
    public   static   final   OntClass   Cognitive_Domain   =
m_model.createClass(                       "http://www.owl-
ontologies.com/unnamed.owl#Cognitive_Domain" );

    /** <p>Comprised of computer network attack, computer
network defense, and related
    *   computer network exploitation enabling operations.
Also called CNO. (Approved
    *   for inclusion in the next edition of JP 1-02.)</p>
    */
    public static final OntClass Computer_Network_Operations
=         m_model.createClass(               "http://www.owl-
ontologies.com/unnamed.owl#Computer_Network_Operations" );

    /**   <p>Actions   taken   through   the   use   of   computer
networks to disrupt, deny, degrade,
    *   or destroy information resident in computers and
computer networks, or the
    *   computers and networks themselves. Also called CNA.
(This term and its definition
    *   modify the existing term and its definition and are
approved for inclusion
    *   in the next edition of JP 1-02.)</p>
    */
    public static final OntClass Computer_Network_Attack =
m_model.createClass(                       "http://www.owl-
ontologies.com/unnamed.owl#Computer_Network_Attack" );

    public static final Individual Information_Operations_1
        = m_model.createIndividual( "http://www.owl-
    ontologies.com/unnamed.owl#Information_Operations_1",
          Information_Operations_Resources );}
```

LIST OF REFERENCES

Alesso, P., & Smith, C. (2005). *Developing Semantic Web Services.* Wellesley, MA.
    A K Peters, Ltd.

Bachimont, B., Isaac, A., Troncy, R. "Semantic Commitment for Designing Ontologies:
    A Proposal," *In Knowledge Engineering and Knowledge Management:*
    Ontologies for the Semantic Web, 13th Annual Conference, Siguenza, Spain,
    2002.

Benjamins, R. and Fensel, D. "The Ontological Engineering Initiative," *Proceedings of
    the International Conference on Formal Ontology in Information Systems*, 1998.

Berners-Lee, Tim. (1999). *Weaving the Web*. New York: HarperCollins Publishers, Inc.

Berners-Lee, T., Hendler, J., & Lassila, O. (2001). *The Semantic Web.* Scientific
    America: May 17, 2001.

Chance, S. and Hagenston, M. *Assessing the Potential Value of Semantic
    Web Technologies in Support of Military Operations*. Monterey, CA: NPS, 2003.

Cross, V. and Pal, A. Metrics for Ontologies. Fuzzy Information Processing Society,
    2005. NAFIPS 2005. Annual Meeting of the North American Fuzzy Information
    Processing Society. 2005.

Childers, C. *Applying Semantic Web Concepts to Support Net-Centric Warfare Using the
    Tactical Assessment Markup Language (TAML).* Monterey, CA: NPS, 2006.

Daconta, M., Obrst, L. and Smith, K. *The Semantic Web: A Guide to the Future of
    XML, Web Services and Knowledge Management.* Indianapolis, Indiana: Wiley
    Publishing Inc. 2003.

Davies, J., Fensel, D. and Van Harmelen, F. *Towards the Semantic Web: Ontology
    Driven Knowledge Management*. West Sussex, U.K.: John Wiley and Sons. 2003.

Dejing Dou, et al. "Integrating Databases into the Semantic Web through an Ontology-
    based Framework" Proceedings of the 22nd International Conference on Data
    Engineering Workshops. 2006.

Dong, J. S. and D. Dan. *Software Engineering Approaches to Semantic Web*. Engineering
    of Complex Computer Systems, 2005. ICECCS 2005. Proceedings. 10th IEEE
    International Conference. 2005.

General Dynamics Advanced Information Systems. *Information Warfare Planning Capability*. Online brochure. Arlington, VA: 2007. URL:<http://www.gd-ais.com>. Accessed May 24, 2007.

Guizzardi, G. *The Role of Foundational Ontologies for Conceptual Modeling and Domain Ontology Representation*. Databases and Information Systems, 2006 7th International Baltic Conference. 2006.

Hepp, M. *Possible Ontologies: How Reality Constrains the Development of Relevant Ontologies*. Internet Computing, IEEE. Vol. 11. 2007.

Hossain, M. A., A. El Saddik, and P. Levy. *Towards a Multi-Domain Semantic Web Application*. Electrical and Computer Engineering, 2004. Canadian Conference Vol. 32004.

Jane's Intelligence Centres. << http://www8.janes.com.libproxy.nps.edu/Search/documentView.do?docId=/content1/janesdata/yb/jav/jav_1299.htm@current&pageSelected=allJanes&keyword=tank&backPath=http://search.janes.com/Search&Prod_Name=JAV&keyword= >>. Accessed 26 March 2008.

Jiehan Zhou, J. -P Koivisto, and E. Niemela. *A Survey on Semantic Web Services and a Case Study*. Computer Supported Cooperative Work in Design, 2006. CSCWD '06. 10th International Conference. 2006.

Joint Chiefs of Staff. Joint Publication 3-13. *Information Operations*. Washington, DC: GPO, 13 February 2006.

Joint Chiefs of Staff. Joint Publication 3-13.1. *Electronic Warfare*. Washington, DC: GPO, 25 January 2007.

Joint Chiefs of Staff. Joint Publication 3-53. *Doctrine for Joint Psychological Operations*. Washington, DC: GPO, 5 September 2003.

Jones, C. "Patterns of Large Software Systems: Failure and Success." *Computer* 28, no. 3 (1995): 86-87.

Jones, C. *Patterns of Large Software Systems: Failure and Success*. Computer. Vol. 281995.

Lacy, L. *OWL: Representing Information Using the Web Ontology Language*. Canada: Trafford.

Liang Chang, Fen Lin, and Zhongzhi Shi. *A Dynamic Description Logic for Semantic Web Service. Semantics, Knowledge and Grid*, Third International Conference on Semantics, Knowledge, and Grid. 2007.

Mannes, A. and J. Golbeck. *Ontology Building: A Terrorism Specialist's Perspective*. Aerospace Conference, 2007. IEEE 2007.

Maedche, A. *Ontology Learning for the Semantic Web*. Boston, Massachusetts: Kluwer Academic Publishers. 2002.

Mena, E. V., Kashyap, A. Illarramendi, and Sheth, A. "Domain Specific Ontologies for Semantic Information Brokering on the Global Information Infrastructure," *Proceedings of the International Conference on Formal Ontology in Information Systems*, 1998.

Noy, N., & McGuinness, D. (2001). *Ontology Development 101: A Guide to Creating Your First Ontology.* <http://protege.stanford.edu/publications/ontology _development/ontology101-noymcguinness.html.> Accessed September 1, 2007.

Office of the Under Secretary of Defense For Acquisition, Technology and Logistics. *The Creation and Dissemination of All Forms of Information in Support of Psychological Operations (PSYOP) in Time of Military Conflict*. Report of the Defense Science Board Task Force. Washington, D.C., May 2000.

Pan, Jeff Z. *A Flexible Ontology Reasoning Architecture for the Semantic Web*. Knowledge and Data Engineering, IEEE Transactions. Vol. 192007.

University of Manchester and University of Karlsruhe. "WonderWeb OWL Ontology Validator." <http://www.mygrid.org.uk/OWL/Validator>. Accessed May 15, 2008.

U.S. Army War College, Dept. of Military Strategy, Planning, and Operations. *Information Operations Primer: Fundamentals of Information Operations.* Carlisle, PA. 2006.

Wilson, M. and B. Matthews. *The Semantic Web: Prospects and Challenges*. Databases and Information Systems, 2006 7th International Baltic Conference. 2006.

World Wide Web Consortium. "W3C Validation Service." <http://www.w3.org/RDF/Validator/>. Accessed May 15, 2008.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1.   Defense Technical Information Center
        Ft. Belvoir, Virginia

2.   Dudley Knox Library
        Naval Postgraduate School
        Monterey, California

3.   Man-Tak Shing
        Naval Postgraduate School
        Monterey, California

4.   LtCol Karl Pfeiffer
        Naval Postgraduate School
        Monterey, California

5.   Dr. Dan Boger, Information Sciences Department Chairman
        Naval Postgraduate School
        Monterey, California

6.   Dr. Peter Denning, Computer Science Department Chairman
        Naval Postgraduate School
        Monterey, California